SCALE COMPUTING

Implementing Business Resilience Best Practices

An essential guide to preparation from an I.T. perspective

Solutions Brief

Table of Contents

Introduction

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

This paper is intended for organizations of all kinds and of all sizes to provide guidance on how to best prepare for business resilience from an information technology perspective. These best practices will highlight current technologies that can 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 all have probably thought of business resilience by other names such as risk management, emergency management, business continuity, disaster recovery planning, and risk mitigation. Business resilience looks to be a broader approach to including all of these types of planning with a focus on how to continue organizational success when there are issues that 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 type of organization benefits from business resilience. Business resilience, despite what may be inferred from the name, is not just for commercial businesses. Governmental organizations, both local or 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 provide services that are relied on in many communities and these organizations benefit from business resilience to ensure those services may continue.

Which business operations are critical to organizational success?

This depends entirely on the type of organization and in some cases the level of disruption. For a hospital, for example, a majority of operations may be critical and need to continue in some capacity. For police and fire departments, the ability to respond to emergencies is extremely critical for the safety of the community. For a small commercial business, it may only be critical to ensure employees are safe and that the business can effectively communicate both internally and externally to keep employees and customers updated until business services can resume.

What are the disruptive events business resilience addresses?

Organizations are at risk of 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 outage. Current events have demonstrated that many organizations were not nearly adequately prepared for a global pandemic nor were many organizations prepared to handle the increase in cyberattacks like ransomware.

Some organizations have specific planning needs toward certain types of typical regional natural disasters such as earthquakes, floods, or hurricanes based on where their offices are physically located. However, all organizations must prepare more generally for almost any type of potential threat, and planning should take into account the severity of different threat levels. The planned steps needed to deal with fire in the building will certainly be different from the planned steps needed to deal with a ransomware attack or a server failure.

What are the elements of business resilience?

In the broad sense, business resilience extends well beyond the IT department and includes many elements such as brand protection, building evacuation plans, ensuring the organization has adequate insurance policies in place, setting aside cash reserves for emergency funds, and having communication plans in place for employees 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 - Protection, mitigation, and recovery from cyber attacks.

Business Resilience in the Data Center

The data center is the heart of IT operations. Without the data center, data and applications are disconnected between departments, teams, and individuals. The organization struggles to work as a whole when the datacenter cannot connect all of the organization's parts fluidly through the flow of data. There are many aspects of data center resilience that must be considered.

Data Backup

Perhaps the oldest and most prominent element of business resilience is backing up data. Next to the 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. Having a data backup has been and will likely continue to be one of the most basic and necessary elements of business resilience.

However, one side of data backup that is often lacking in business resilience planning is the proper testing of data backups. Testing allows an organization to ensure both that data is properly being backed up and that the recovery process for that data aligns with the recovery time objectives required should recovery be necessary. Without testing of data backups, organizations take a big risk when it comes to recovering at the point of data loss.

Disaster Recovery (DR)

Beyond data backups, organizations should have in place 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 that it 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 at 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 data in order for the DR site to effectively stand-in for the data center. 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 a matter of 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 do not have to change their own 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 measure and an important one, especially when an organization experiences an entire site outage at the primary data center. However, failing over to a DR site is not always necessary particularly if only a single server or application fails. For more localized disruptions within the data center, high availability is a preferred solution.

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 where 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 nearly eliminate system downtime, reducing it from hours or even days to only a few minutes.

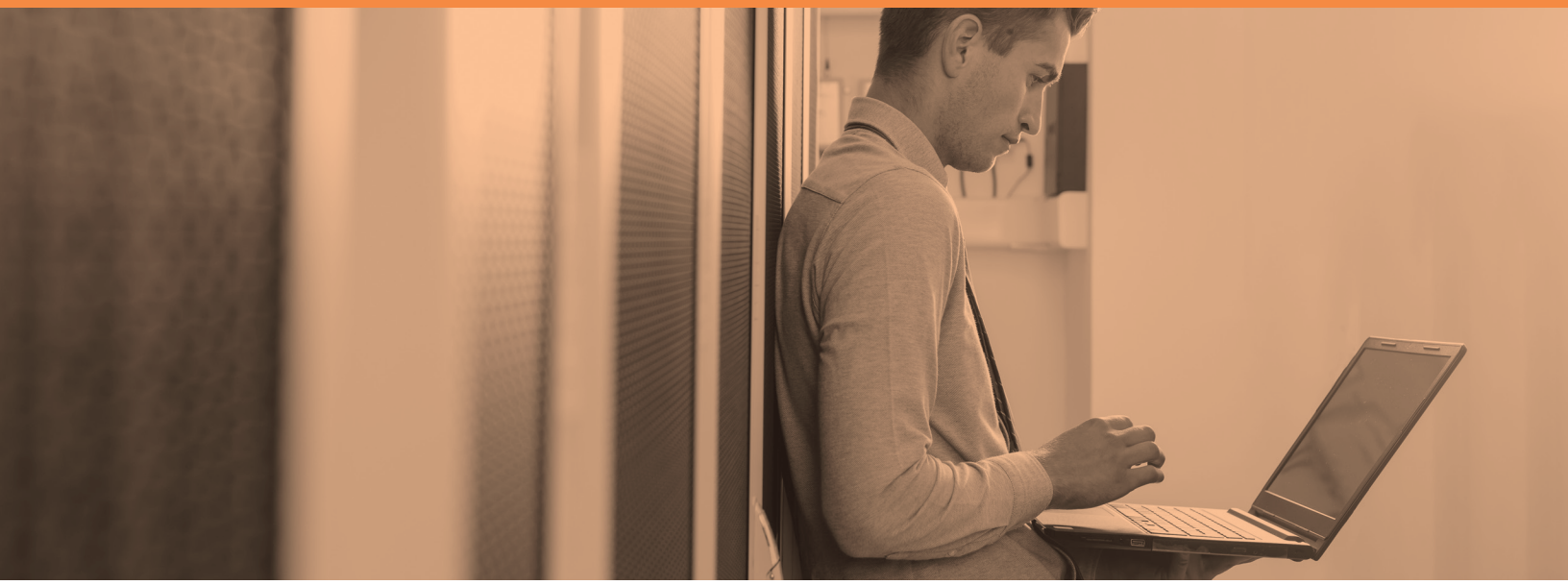
Some high availability clusters can be geographically dispersed across sites, however, the high-speed networking requirements for such "stretch" clusters to allow them to operate across sites effectively can easily make them cost-prohibitive to many organizations. Failing over between sites generally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

Planning and Testing

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

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

As mentioned earlier in regards to data backups, testing is an essential part of ensuring successful business resilience. A plan is only as good as the ability of the staff to execute it. Periodically updating the plans and testing the plans are essential to having confidence that the plans will be successful when needed. A best practice for testing is to execute a real-time test for business resilience once or twice a year.



Personnel, Training, and Expertise

When an organization faces an outage, disruption, or disaster no business resilience planning is going to succeed without the assistance of the IT staff and their unique skills. Depending on the size of an organization, the IT staff may range in size from a single IT generalist to a large team or teams of IT specialists. The size of the organization will also most likely determine the complexity of both the IT systems and the 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 business resilience plans can be available in the time of need. To accomplish this in a large, medium, or even a small team with specialized IT professionals, 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 the agreements they have with their service providers or consultants match their organizational goals for business resilience. Further, these organizations should make sure that business resilience plans can be tested and executed successfully when needed. It is also important to determine how regional disasters may impact service levels from these service providers and consultants if they too are affected by the disaster.

Data Security

This paper will cover some data security topics such as workstation security and cyber security in later sections. In this section, we'll discuss some practical steps that can be implemented for business resilience.

Physical security of systems can be extremely important. Organizations store sensitive data that must be protected to comply with regulations or must be protected to protect the intellectual property and trade secrets needed to be competitive. Organizations can't afford to allow any employee to wander into the data center with the possibility of walking out with a stolen or copied hard drive, for example. Physically restricting who can access the primary computing systems physically can prevent both theft and vandalism of data.

Network and application security is also very important. Employees and even customers should only be able to access limited sets of data that they need to perform their work or do business. A user who accesses data outside of their normal job responsibilities may not be aware of the sensitive nature of the data and 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 important 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 be using 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 and should never fail, but in reality, even the biggest cloud services fail from time to time.

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 that are deemed critical may require redundancies on-premises to ensure that they will be available in the event of the cloud or internet outage. Additionally, cloud applications and services should be integrated into business resilience testing, particularly 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 the work of the organization. When users cannot access the data and applications they need, the business of the organization can slow dramatically or stop completely. 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 a worker may use to run the applications and access the data they need to work. These can be in the form of desktop computers, laptops, tablets, mobile phones, or other more specialized digital devices.

Working Remotely

In 2020, the COVID 19 virus caused organizations to restrict worker access to offices and other workplaces. Many of these organizations were not prepared to quickly transition user workstations to work from home. Traditional thinking of providing employees with a desktop computer at their office desk did not allow for a quick transition to remote working. While some organizations located in regions with frequent natural disasters might have already incorporated work-from-home strategies into their business resilience planning, 2020 established that nearly all organizations need to plan for it to some extent.

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

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

Device Management

How workstations are supported by the IT team 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 of time, how quickly can the IT department address issues with those devices remotely to maintain productivity? How quickly can IT roll out necessary security patches or hotfixes or new applications if so many employees are now remote?

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

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

Data Security

Workstation devices pose a number of security risks to organizations. Firstly, they are set up to connect to an organization's data and applications so a workstation device getting into the wrong hands is a concern for a data breach or malicious tampering of data or systems. Next, users may not always follow security best practices when it comes to operating these devices which makes workstations a key vulnerability to cyber attacks. Finally, as workers work remotely from home or other less secure networks using VPN, they extend the organizations network out to these less secure networks increasing vulnerability.

A data breach or cyber attack infiltrating through a vulnerable workstation can have severe consequences for an organization. A ransomware attack originating from a user workstation can nearly cripple an entire IT system and the business that runs on it. Addressing workstation security vulnerabilities involves a combination of making sure devices have strong authentication mechanisms in place especially if they are being used in the field, making sure their are strong antivirus protections in place on the devices, and making sure users are properly trained on best practices to avoid data security issues.

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

Cyber Security

Cyber security and cyber attacks are part of an arms race that has been going on since the beginning of the internet and there appears to be no end in sight. Instead, both attacks and security measures designed to stop attacks are becoming increasingly sophisticated both technologically and tactically. A combination of proactive and reactive measures are required to successful combat cyber attacks as part of business resilience.

Proactive Security Measures

Proactively, this paper has already discussed some physical security measures around access to the data center as well as restrictions on data access for system users. This paper has also discussed proactive measures relating to the security of workstations. Yet additional steps can be taken to harden an organization's IT systems and to counteract security threats as they are occurring.

Firewalls and gateways can restrict external access and have been in use for decades to harden computing networks by reducing the surface area of attack. These are still important to monitor and review for vulnerabilities. Anti-virus scanners are also important to examine data, especially incoming data, for a wide variety of cyber attacks 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 can not only detect and stop attacks but actively roll back the damage done by these attacks in real-time.

One thing in common for all IT systems and security solutions is that timely updates and patching are needed to maintain good security. Security scanners are only as good as the types of threats they are programmed to detect. Application vendors often respond quickly with security patches to new threats 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 in an important part of business resilience.

Training is also a key part of proactive security measures. Training IT staff on security best practices is important but it is equally important to train users on security best practices. 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

It is likely a question of **when** rather than if an organization will get hit with a cyber attack, despite its best efforts to avoid it. When an attack does occur, whether it is a data breach or a ransomware attack, it is important to have a plan on how to handle that occurrence. The more quickly an organization can respond, the less damage they may face from the attack.

Data 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. Some cyber attacks are becoming more sophisticated, however, and lying dormant for weeks or months before becoming active and "attacking". In these cases, reverting back a few hours or even days 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. As much as can be possible, organizations should train workers on what they should be doing in the event of a cyber attack of some kind. Waiting to communicate these instructions until after the attack may be too late. For example, if files become infected and an organization becomes aware of the attack, users should know not to continue distributing files across various systems which can spread the infection further. Proper training, data backups, and snapshot are absolutely good to have for a number of reasons regarding lost or corrupted data but 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

The Scale Computing HC3 hyperconverged infrastructure platform was practically designed and built for business resilience. With native high-availability clustering, built-in disaster recovery features, and intelligent, automated self-healing capabilities, the HC3 platform is so reliable it practically eliminates downtime. Our HC3 platform can be deployed quickly, managed easily, and scaled out seamlessly and flexibly. Find out more about the HC3 platform **here** on the Scale Computing website.

Virtual Desktop Infrastructure

Scale Computing VDI solutions are built around our easy-to-use and highly available HC3 platform to deliver an equally easy and cost-effective VDI experience. With flexible bring your own device (BYOD) support and full life cycle management capabilities for virtual workstations, VDI solutions from Scale Computing are not just easy to implement but can be sized to support organizations of any size, even the small and midmarket organizations that might have thought VDI was too big an investment in the past. Find out more about Scale Computing VDI solutions **here** on the Scale Computing website.

Ransomware Protection

Scale Computing offers Acronis Cyber Backup solutions with active ransomware protection features and a full complement of advanced data backup capabilities. Acronis actively monitors virtual machines and can detect ransomware attacks as they are occurring and automatically roll back ransomware infections in real-time. Acronis is not only a smart choice for ransomware protection but also a powerful backup solution for data protection and recovery. Find out more about Acronis solutions from Scale Computing **here** on the Scale Computing website.

Summary

In an increasingly digital world with ever-present threats that can disrupt business operations, every organization should make business resilience an essential part of their 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 is a combination of proactive and reactive plans that make an organization viable through a wide range of challenges, disruptions, and disasters. Business resilience can prevent small disruptions from becoming huge disruptions and can prevent catastrophic disasters from becoming fatal to the organization's existence. Organizations need to take business resilience seriously and make sure the appropriate level of effort is being given against the possible threats that may occur.

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

Introduction to Virtual Desktop Infrastructure White Paper

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