infopulse

eBook

Business Continuity and Disaster Recovery: How to Protect Your Business_

Table of Contents

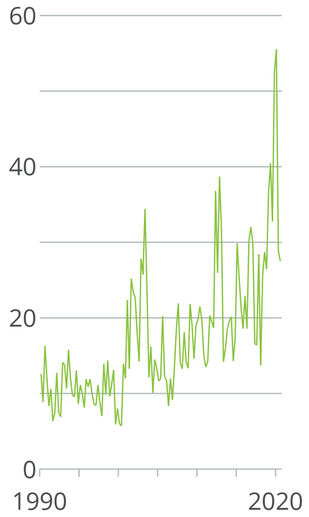
From supply chains to information flows, businesses today are more interconnected with one another than just a decade ago.

However, a greater degree of connectivity also expanded corporate risk radars. A temporary power outage in one region can leave hundreds of businesses paralyzed. When more adverse events happen – ranging from social instability to natural disasters and cyber-attacks – their impacts can cause a ripple effect of disruption across industries.

Soundly, most companies today choose to plan ahead for disruption, rather than wait for it to strike and put down business continuity and disaster response plans.

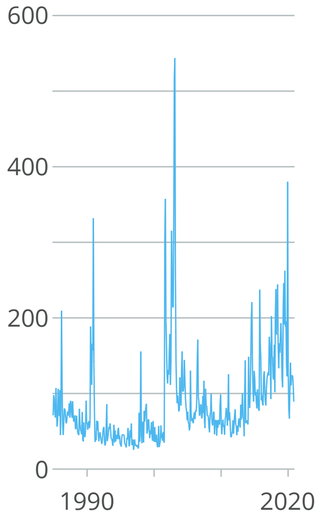
Disruption is becoming more frequent and more severe

IMF World Uncertainty Index*, thousand



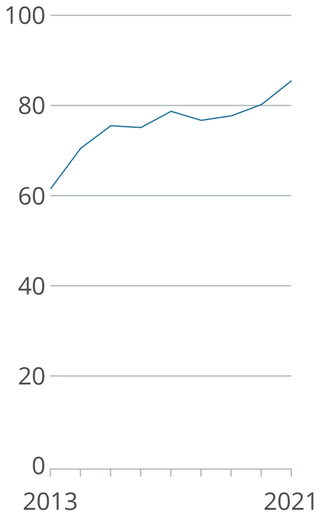
Global uncertainty has grown manifold since 2000

Federal Reserve Board, Geopolitical Risk Index**



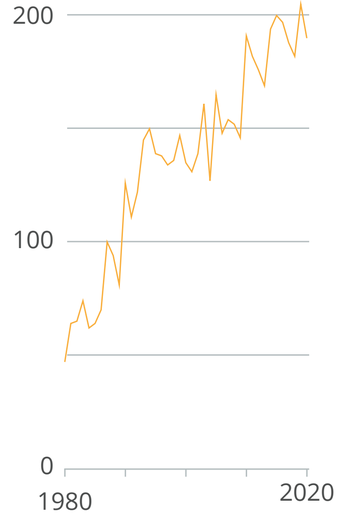
Geopolitical risk has not been higher since 2003

Companies subject to a cyber breach per year, %



Cyber incidents have risen 24 percentage points since 2013

Natural disasters per year, number



Frequency of natural disasters is rising

* Based on the percentage of the word “uncertain” (or its variant) in the Economist Intelligence Unit country reports.

** Automated text-search results from the electronic archives of 11 newspapers: Boston Globe, Chicago Tribune, Daily Telegraph, Financial Times, Globe and Mail, Guardian, Los Angeles Times, New York Times, Wall Street Journal, and Washington Post. Index was calculated by counting the number of articles related to geopolitical risk in each newspaper for each month (as a share of the total number of news articles).

Source: CyberEdge; Swiss Re

Source

infopulse

What is Business Continuity (BC)?_

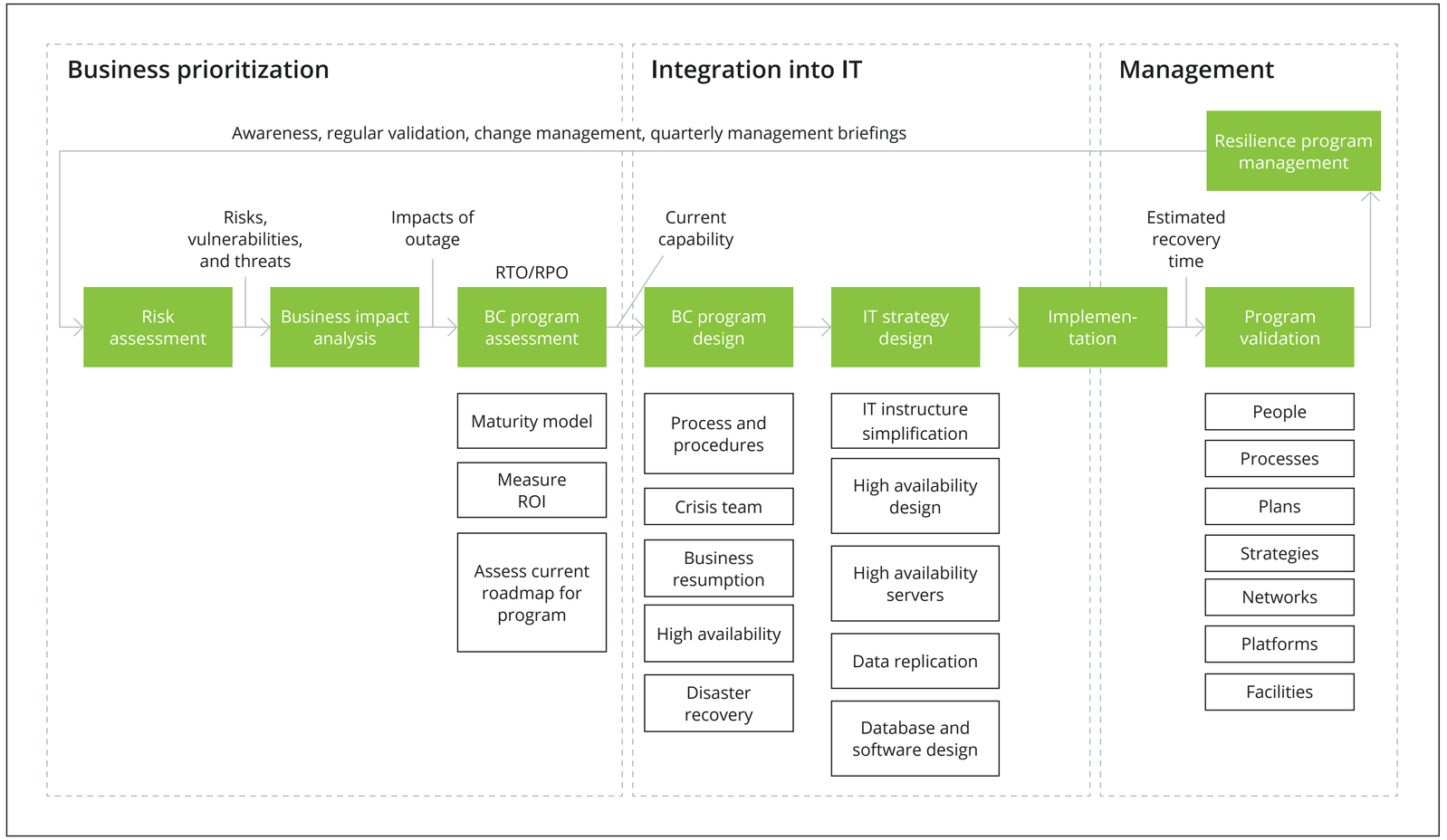
Business continuity (BC) is the ability of an organization to continue operations after a force majeure event (e.g., a cyber-attack, data breach, natural disaster, etc.).

The global pandemic has put businesses to a stress test but also proved that many had grossly overestimated their preparedness for disruptions. In March 2020, Garter reported that 12% of enterprises considered themselves highly prepared for Covid-19 and 56% rated themselves as somewhat prepared[1]. Yet, by mid-August 2020, 80% of board members had to admit that their firms were not well-prepared for an adverse event such as the global pandemic[2].

The change of sentiment is hardly surprising when you look at the underlying facts. Globally, only 53% of organizations had a formal business continuity plan (BCP) in place before Covid-19 hit[3].

A **business continuity plan (BCP)** is a formal set of actions, practices, and procedures, designed to ensure the fast resumption of essential business functions after an unplanned disruption.

A Business Continuity Planning Process



Source

[1] Gartner Business Continuity Survey Shows Just 12 Percent of Organizations Are Highly Prepared for Coronavirus. Gartner. Retrieved August 15, 2022

[2] Nearly 80% of Board Members Felt Unprepared for a Major Risk Event Like COVID-19: EY survey. EY. Retrieved August 15, 2022.

[3] A global survey of enterprises: Managing the business disruptions of COVID-19. International Labour Organization. Retrieved August 15, 2022.

A BCP has three primary objectives:

1. Ensure high resource(s) availability	2. Maintain undisrupted operations	3. Disaster recovery
Despite the disruption, a company can maintain access to critical business systems, applications, and data to continue its operations. The plan includes mitigation paths and alternative operating procedures if a failure occurs within physical facilities, IT infrastructure, or business processes.	The company can continue to function as usual thanks to pre-planned damage mitigation steps, checklists, and procedures.	In case of technical disruption, the company can recover its data center and business applications from an alternative site without incurring any data losses.

Components of a Business Continuity Plan

- Operational strategy
- Organizational plans
- Processes optimization
- Facilities management
- Application and data availability
- BC and DR technologies

infopulse

What is Disaster Recovery (DR)?_

Disaster recovery (DR) is a standardized process for regaining access to IT infrastructure after a disruptive event. It includes both operational policies and technological methods for restoring normal IT operations.

IT infrastructure, which now includes on-premises hardware, public and private clouds, corporate networks, business applications, and data centers, has become a pivotal enabler for business continuity. Yet, because of technology's fundamental role in corporate operations, IT infrastructure is also a "weak link".

Human errors, power outages, or sophisticated cyber-attacks can leave companies fully paralyzed. Last year, we saw Facebook, Instagram, and WhatsApp going down simultaneously for hours because of an error in DNS configurations. Or there is an earlier Vodafone case of receiving a £4.6 million regulatory fine after a poorly executed CRM system migration they could not roll back[4].

Disasters of a smaller scale occur every other day. However, only 54% of organizations had a documented company-wide disaster recovery strategy. Even though 73% of respondents experienced a technical failure event at some point[5]. At the same time, companies with DR plans in place still lack full confidence in their current setup. IDC reports that only 13% of organizations have full confidence in their backup system's ability to recover data and 20% are completely certain in their DR solution[6].

Disaster recovery plans (DRPs) include all practices, policies, and technologies a company has in place to ensure the fast restoration of IT systems, services, applications, and data.

Only 54% of organizations have a documented company-wide disaster recovery strategy

[4] Vodafone's £4.6m CRM fine - when IT projects attack. Diginomica. Retrieved August 15, 2022.

[5] Only 54% of organizations have a company-wide disaster recovery plan in place. Security Magazine. Retrieved August 15, 2022.

[6] The State of Data Protection and Disaster Recovery Readiness: 2021. IDC. Retrieved August 15, 2022.

A DRP has three primary objectives:

1. Keep core operations as uninterrupted as possible DRP documents a set of processes and technical facets for ensuring alternative means of operation in advance.	**2. Provide consistent and rapid restoration of IT services,** thanks to documented procedures and pre-implemented services failover, data redundancy, and systems' backup mechanisms.	**3. Limit the impacts and damage of disruptions** through a rapid recovery process, proactive risk management, and impact minimization strategies.

Components of a Disaster Recovery Plan

- IT backup and off-site storage procedures
- Risk/impact assessment matrix
- Disaster action checklist
- Recovery startup procedures
- Roles and responsibility matrix
- DR plan training and testing policies

infopulse

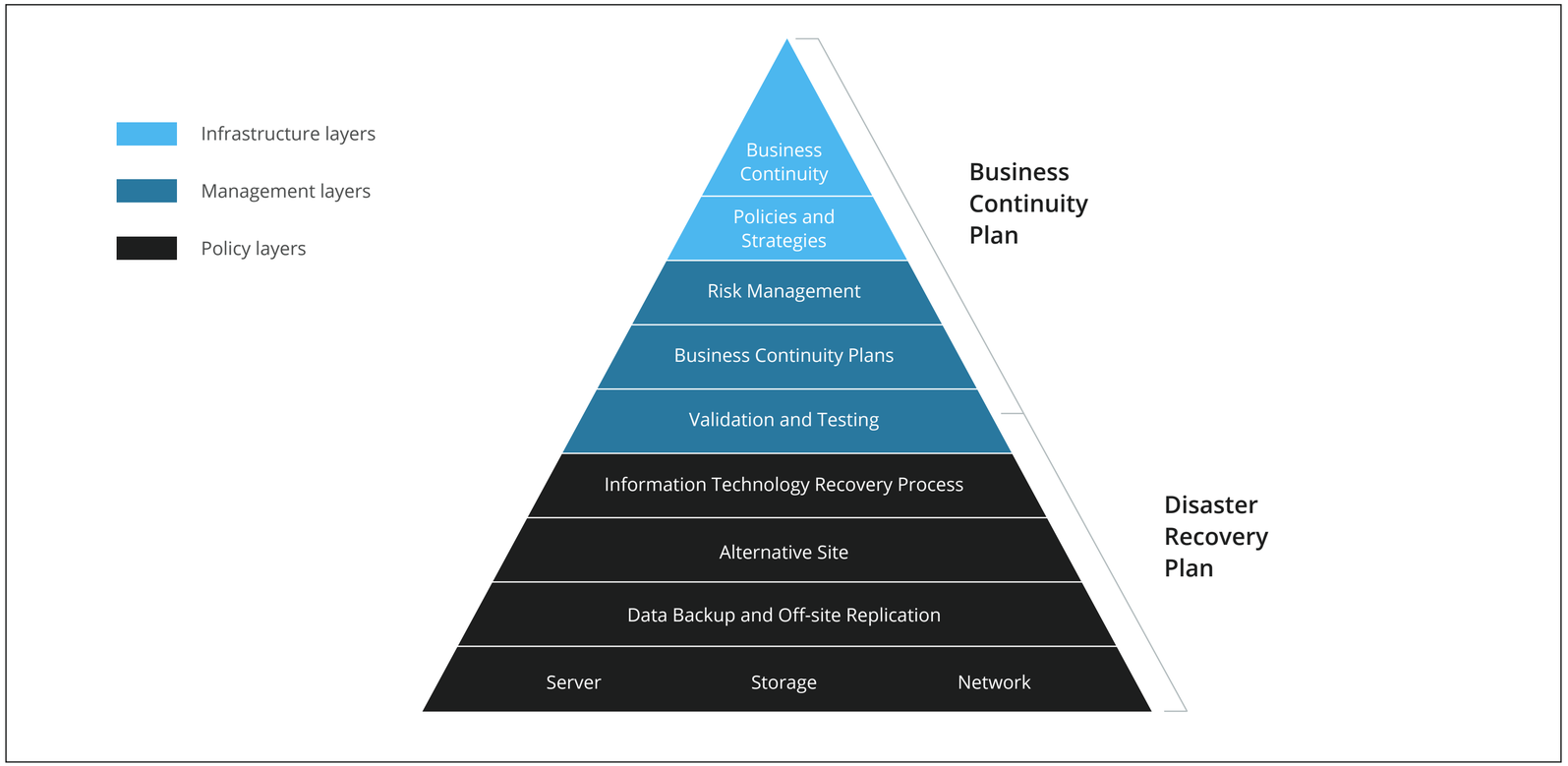
What is BCDR?

Disaster recovery has become an integral part of business continuity plans as people's dependency on technologies reached unprecedented levels.

Because continuous corporate operations have become almost synonymous with stable IT infrastructure performance, BC and DR activities now merged into a consolidated business continuity-disaster recovery (BCDR) plan.

As such, it covers technology, operational, and policy procedures that must be in place for effective business roll-back to operations as usual.

Business continuity and disaster recovery planning



"The reason why the Ukrainian government and a lot of critical infrastructure is able to continue to function in a very resilient way is thanks to the cloud infrastructure. In fact, we were able to work with the Ukrainian government, migrate their systems, and in some sense have continuity. So, cloud is becoming more and more ubiquitous. And another great example [is from] NASA for the International Space Station. They need to keep the integrity of the suits very high. [...] You can't have any malfunction. So, they have now computation that is happening in the space station because the latency is too high. So, the infrastructure itself, thanks to 5G, thanks to space, is really spreading everywhere...

Satya Nadella

CEO of Microsoft

infopulse

The Need for the BCDR in the Digital-First, Post-COVID Era_

Over 2,8 billion malware attacks were recorded globally since the beginning of 2022

The pandemic has given many business leaders greater confidence in their operational resilience. Indeed, organizations worldwide have shown admirable creativity, tenacity, and fortitude in maintaining business as usual or rapidly pivoting to new operating models.

Many have since evolved the “temp” practices of “remote work” and “cloud-first thinking” to become a permanent element of their businesses. Almost every industry advanced five years forward in terms of digitization in a span of several months[7].

However, the opposite side of rapid digitization (which carried many benefits) is the increased dependency on uninterrupted connectivity, low-latency data transmissions, and data redundancy. The sophistication and proliferation of cyberattacks also put a strain on corporate protection. **Over 2,8 billion malware attacks were recorded globally since the beginning of 2022** — and ransomware rates in Europe spiked by 63%[8].

That said, human error and hardware failure are the reasons behind almost 55% of data losses[9]. Unlike cyber-security (which is often a separate area of responsibility, covered by SOC teams), these two cases are often underlooked by businesses.

In April 2022, Atlassian experienced a two-week outage, affecting over 775 customers, who were fully locked out of their accounts. The after-action analysis revealed that the engineers ran a script to remove legacy data as part of the scheduled maintenance. However, an error in the script led to wider data removal. The event could have had worse consequences if not for Atlassian’s extensive backup and recovery systems. No customer data was lost and all services were restored to normal[10].

Increased traffic volumes also put a greater strain on aging local infrastructure. The frequency of server failures increased from 5% in the first year to 18% in the seventh year[11]. Yet, many companies do not rush to retire or upgrade legacy infrastructure – a factor that also increases operational risks.

> The **role of BCDR** is to minimize the chances and effects of possible disruptions on business operations, whether these are of technological, human, or physical nature.

[7] Global surveys of consumer sentiment during the coronavirus crisis. McKinsey. Retrieved August 15, 2022

[8] 2022 SonicWall Cyber Threat Report. SonicWall. Retrieved August 15, 2022.

[9] Data Health Check 2021. Databarracks. Retrieved August 15, 2022.

[10] Post-Incident Review on the Atlassian April 2022 outage. Atlassian. Retrieved August 15, 2022.

[11] Frequency of server failure based on the age of the server. Statista. Retrieved August 15, 2022

infopulse

BCDR Business Cases_

By implementing BCDR practices, an organization can quickly recover after an adverse event, minimize the risk of data loss, reputational damage, and compliance fines; and maintain high operational resilience even in uncertain times.

In this section, we discuss different business cases for implementing BCDR technologies for small, mid-market, and enterprise-sized companies across industries.

Small and Medium Businesses (SMBs)

Statistically, SMBs tend to have more lax attitudes towards BCDR: 43% admit to having no current BCP plan in place and no intention to implement one[12]. More often than not, it proves to be a huge oversight.

On average, employees of a small business (below 100 people) tend to experience 350% more social engineering attacks than employees of a larger enterprise. As a result, **one in five organizations had at least one account compromised last year[13].** Separately, some 56% of employees admitted to accidentally deleting cloud records, 43% of whom chose not to disclose this fact to their superiors[14].

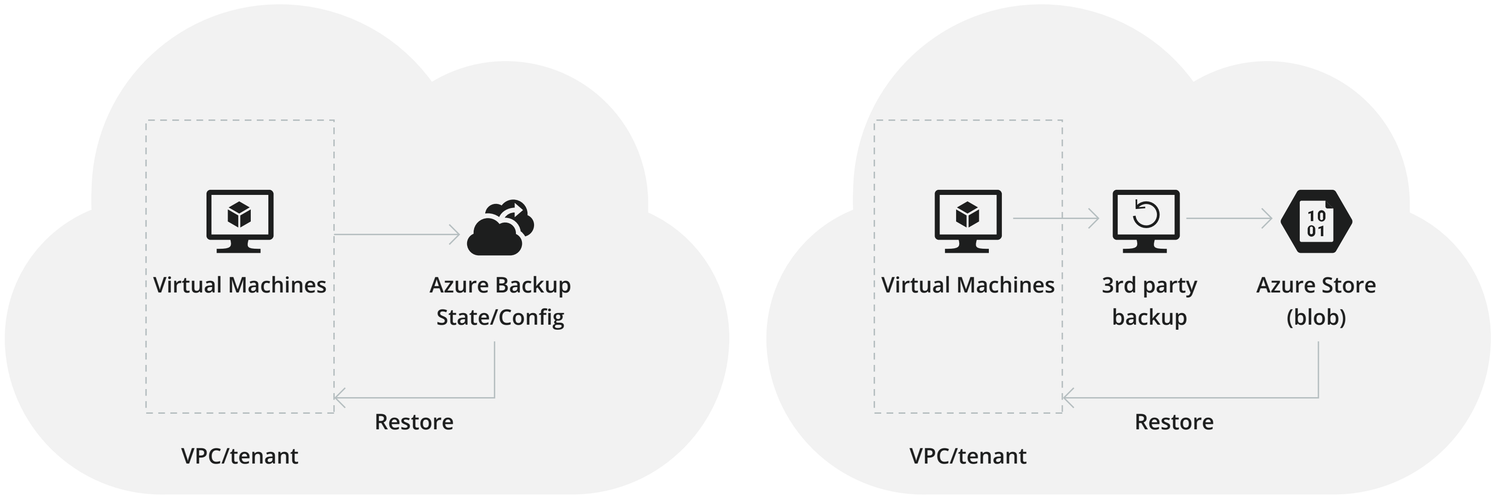
For SMBs, even the simplest BCDR architecture can act as a "safety net", protecting them from substantial financial and reputational losses in case of an adverse event. With the average cost of a data breach for SMBs sitting at $108K[15], investments in BCDR pays themselves manyfold – and generate ROI afterward.

[12] Data Health Check 2021. Databarracks. Retrieved August 15, 2022.
[13] Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies. Forbers. Retrieved August 15, 2022.
[14] Report: 56% of workers admit they've accidentally deleted cloud data. VentureBeat. Retrieved August 15, 2022.
[15] Security for your small or medium-sized business. Microsoft. Retrieved August 15, 2022.

Scenario 1. Create a cloud backup for essential services_

Undisrupted access to critical business systems – from digital workplace applications to document management systems – is essential for normal operations. Disaster Recovery as a Service (DRaaS) solutions such as Azure Backup allow you to back up asynchronously applications and data to the cloud. Then, if an accident occurs, you can restore access to essential systems in a matter of hours, if not minutes.

Note: *In this scenario, you are only backing up certain business applications and data, not all your IT infrastructure, meaning you might not have access to all of your resources in case of a large-scale IT failure or incident at your physical facility.*



Architecture components

Azure Backup is a centralized data backup service and a collection of supporting services for automating backups of infrastructure, databases, and storage workloads. With it, you can create a comprehensive set of policies for automatic backups and data security.

Supports:

- Azure Virtual Machines
- On-premises servers
- SQL Server
- SAP HANA on Azure Virtual Machines
- Azure Files
- Azure Database for PostgreSQL.

Third-party service + Azure Blob Storage. Alternatively, you can use a third-party data backup solution (e.g., Commvault) to set up database and application backups to Azure Blob Storage. Azure Blob Storage is a scalable cloud data platform, offering multi-protocol access, geo-replication, and top-notch security. Scalable on-demand, Blob Storage can be designated as a hot backup site (for instant data availability) and a cold site for less crucial applications and archival data backups.

Scenario 2. Adopt recommended DR infrastructure_

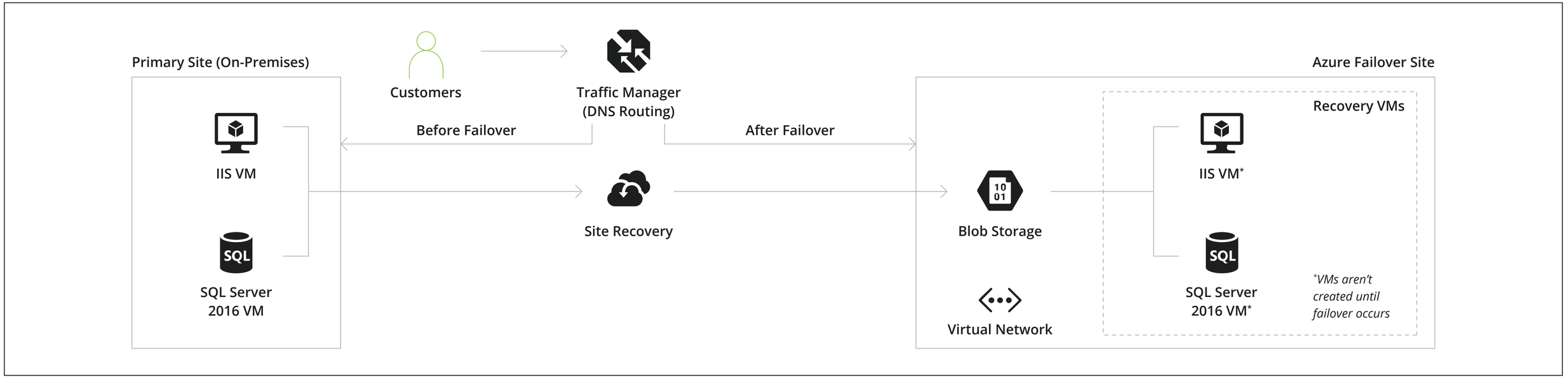
For more critical business data and applications, you might want to achieve full system redundancy (i.e., up to 99.999% uptime at any given period). For example, as an Agro trading company, you might need high IT systems available for all commodity trades and accounting — or you otherwise risk making subpar decisions.

Likewise, always-on IT systems availability is a given for healthcare applications, AdTech solutions, or video streaming services as that is what end-users expect by default. In such cases, implementing services failover is the optimal path forward.

> **Failover** is a backup operation that automatically switches to a standby database, server, or network if the primary one fails or needs to be repaired.

Failover implementation helps you protect your databases during planned maintenance or a system failure. For instance, if a hardware failure occurs in the main on-premises server, a cloud service can immediately take over. Automated switchover also allows you to do planned maintenance without any impact on application performance and offers effective protection against cyber risks.

Azure provides a host of tools for implementing various failover scenarios for cloud, hybrid, and on-premises architectures.



Architecture components

Traffic Manager is a DNS-based load balancing solution for routing traffic between different services. In a DR scenario, Traffic Manager re-directs incoming DNS requests from the primary site to the secondary (failover) site in a matter of seconds. You can either implement a manual failover (i.e., when an engineering team decides to activate your failover site and then re-route traffic) or program automatic failover.

Manual failover is a more common scenario among SMBs as it has lower DR infrastructure costs. In this case, you maintain your secondary site in cold standby, meaning your infrastructure is not active until there is a need for failover. Then you pay for commissioned storage and computing resources when the secondary site is active only.

However, automatic failover might be recommended for systems requiring minimal latency and high availability (such as connected healthcare applications or financial apps). In this case, Traffic Manager sends all traffic to the primary site by default, but if there is any degradation in endpoint performance, Traffic Manager automatically switches traffic to an alternative endpoint. This scenario, howbeit, requires a warm standby site, meaning that the standby site has maximum configurations in place and instances auto-scaling in on. Maintaining such a site is more expensive, yet the benefits are near-real-time recovery point objective (RPO) and recovery time objective (RTO).

Azure Site Recovery is Microsoft-native disaster recovery as a service (DRaaS). As such, it features a comprehensive collection of DR solutions for streamlined replication, failover, and systems recovery.

Site Recovery service replicates physical and virtual machine workloads from the primary to a secondary location. When an incident occurs, all workloads fail over to the designated location and you can access all systems from there. Once the primary site is back up, traffic gets rerouted back to it.

Supports:

- Azure VMs replication between Azure regions
- On-premises VMs, Azure Stack VMs, and physical servers replication to the cloud.

Azure Virtual Network service helps configure a private network infrastructure in the cloud for your failover site.

Blob storage contains the replica images of all machines that are protected by Site Recovery. When a disaster event occurs, Site Recovery initiates failover site generation from the available snapshots.

Enterprises_

Enterprises have bigger data deposits and more critical applications to store and secure. IT systems' availability bar also stands higher as even short-term outages and service latency can translate to multi-million dollar losses.

In 2018, Amazon experienced one of the worst service outages during Prime Day. The company servers could not handle peak traffic load and triggered a cascade of failures. Because of this, Amazon reportedly lost $1.2 million per minute in sales[16].

Disruptions can also happen because of on-site events, ranging from natural disasters to malicious attacks. As many organizations continue to maintain on-premises data centers, these factors should not be overlooked. In 2011, Vodafone suffered a major service disruption after criminals broke into their Basingstoke data center to steal $4 million worth of equipment from the site[17].

To be prepared for both physical and digital threats, enterprise BCDR plans should include a secondary cloud-based data center.

[16] What Amazon lost (and made) on Amazon Prime Day. TechCrunch. Retrieved August 15, 2022.

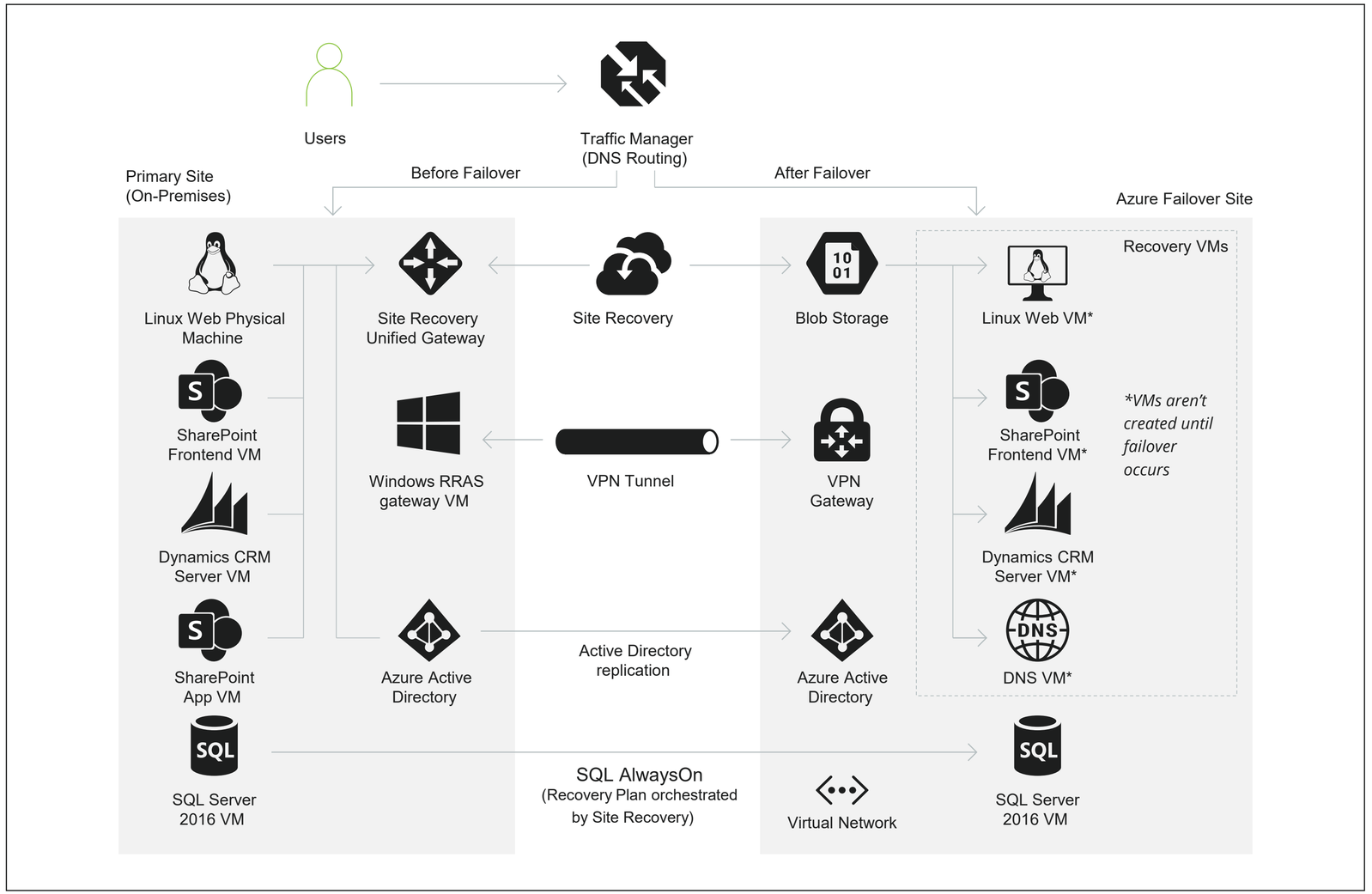
[17] Data centre security: It's time to get physical. Teledata. Retrieved August 15, 2022.

Scenario: Create a secondary data center_

Establishing a secondary data center helps with both disaster recovery and disaster avoidance (critical for business continuity). Apart from serving as a failover site in case of an incident at a primary, cloud-based DR sites in a second availability zone or at a second cloud provider (multi-cloud) can ensure critical business continuity should any regional failures occur.

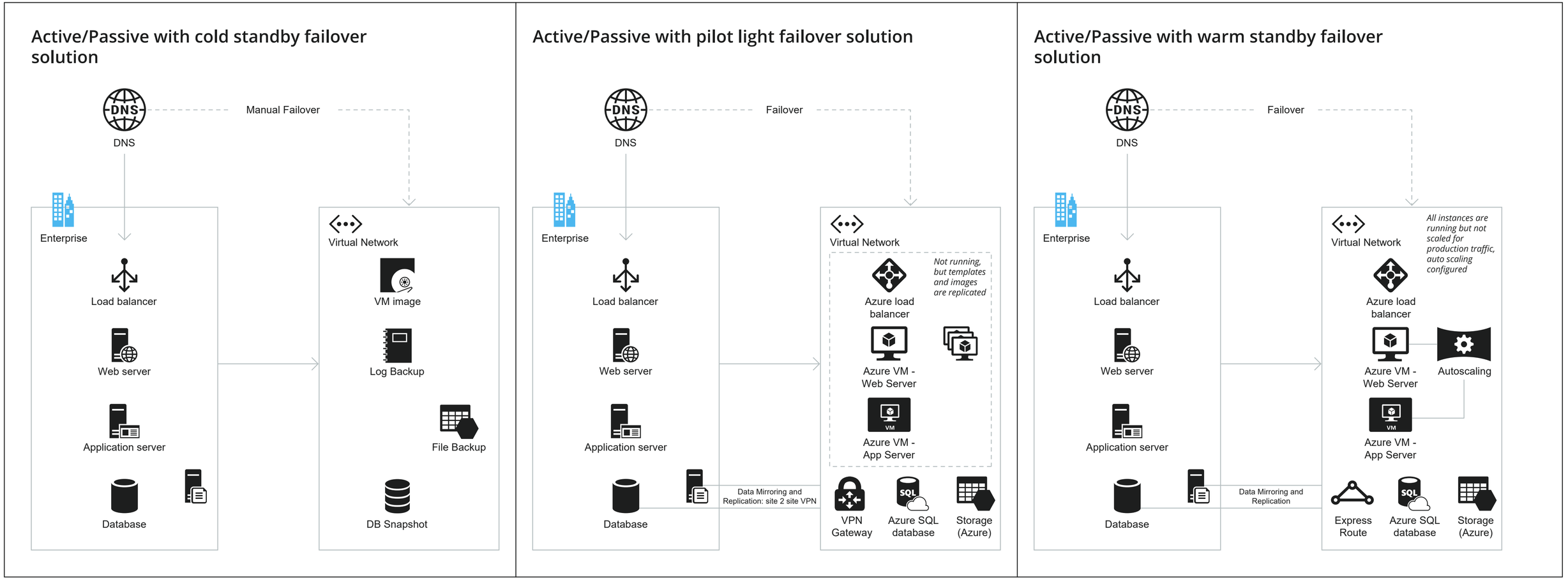
Traditional DR sites (such as NAS storage) mostly require manual activation, data replication, and migration of users. Cloud-based solutions allow the creation of an automated, end-to-end service restoration experience that often takes minutes to activate. Cloud solutions also come with uncapped capacity, meaning you can progressively expand the size of your data center without lengthy hardware procurement cycles or over-paying for currently idle capacities.

Creating a secondary data center with failover to Azure infrastructure is a smart choice for organizations hosting critical data as well as those taking pride in maintaining high end-customer SLAs.



Architecture components

Traffic Manager performs DNS traffic routing from one site to another, based on the codified policies. Depending on your needs, you can implement manual or automatic failover for different disaster recovery scenarios.



Azure Site Recovery DRaaS orchestrates the replication process and manages the configuration of the failback procedures.

Advantages of Site Recovery for Enterprises:

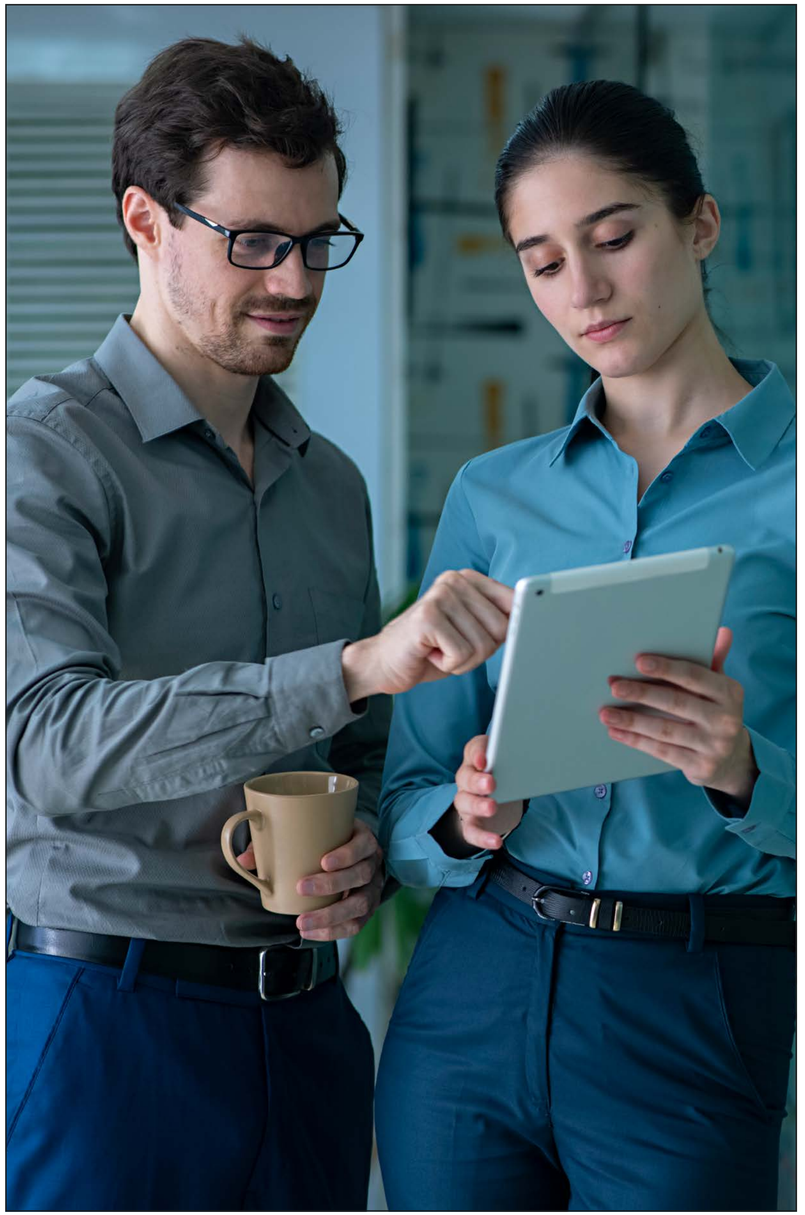
- Data automatically gets stored in Azure elastic storage. Azure VMs are created based on the replicated data.
- Provides continuous replication for Azure VMs and VMware VMs with a replication frequency of as low as 30 seconds.
- Create application-consistent snapshots that capture disk data, all data in memory, and all transactions in process for apps.
- Create customized recovery plans and failover sequences for multi-tier applications running on multiple virtual machines.
- Integrate other BCDR technologies to cover a wider spectrum of applications, databases, and workloads.

All replica images, created by Site Recovery, are stored in **Blob storage** — a scalable, secure cloud storage solution with reserved and on-demand instances available.

To ensure proper security and access management, on-premises **Azure Active Directory** configurations get automatically replicated to the failover site. This way, users can get proper authorizations and accesses to all cloud applications.

VPN Gateway service helps establish a private communication tunnel between on-premises and cloud sites for data replication and subsequent accesses. You can establish point-to-site VPN access from anywhere with a 99.9% uptime. The connectivity is secured by Internet Protocol Security (IPsec) and Internet Key Exchange (IKE) protocols.

Azure Virtual Network solution facilitates the setup of private network infrastructure in the cloud for your failover site. This way, you can additionally secure your site with VPNs or Azure ExpressRoute service. You can also set up isolated and highly secure environments for your most critical databases using firewalls and network security groups (NSGs). Then enable permissioned access to them for users.



infopulse

BCDR at Infopulse_

In 2016, Infopulse began a company-wide BCDR plan preparation and roll-out. By January 2022, we had achieved a 100% test score with all the 46 Product IT systems covered.

In 2019, we have successfully set up a secondary data center in the EU. However, due to the geopolitical events in Ukraine, we decided to convert it into a primary site and successfully migrated most operations to the cloud. As part of this massive shift, we managed to fully migrate our corporate email system to Exchange Online, migrated the internal SharePoint solutions (Infopulse's intranet and department pages) to SharePoint Online, and moved RMS (Rights Management Center) to Azure Information Protection among other sub-projects.

> As a result of the BCP team's proactivity, numerous actions taken in the last 6 years, and the implementation of best practices in business continuity, our engineers managed to deal with all the possible ad hoc scenarios that stunned many businesses during the first two months of war (February-March 2022) in Ukraine. Infopulse now has a hybrid infrastructure that runs like clockwork.

infopulse

How to Embed Security into Your BCDR Planning_

78%

of business executives[18]

Admit to knowing how or when a cyber incident will affect their company.

44%

of the executives[19]

Say that their growing use of partners and suppliers exposes them to significant cyber-security risks.

270

cyber attacks[20]

Occur to one company per year, of which 29 are successful. That's a 31% increase compared to 2020.

Organizations today have to set up a wider defense perimeter, covering cloud, on-premises, and hybrid infrastructure. This proves to be the next security challenge.

Cybersecurity incidents – now occurring with greater frequency – pose another set of disruptions BCDR plans should account for. Nearly every type of business today appears to be an attractive target for cyber-criminals.

The reason is simple — data. The total global data volumes were a "mere" 64 zetabytes in 2020, jumping to 97 zetabytes in 2022[21]. Among those are financial records, citizens' private identifiable information (PII), medical records, and website login credentials — all valuable targets for cyber-attackers.

By getting hold of the corporate data, hackers can either gain control of core business systems (as was the case with the SolarWinds Hack) or steal/encrypt sensitive business data to demand ransomware (as was the case with Cognizant in 2020). In every case, the affected company does not only incur direct damage in form of lost revenue and regulatory fines but also carries major reputational losses. British telco, TalkTalk, lost over 280,000 customers and almost $1.4 billion in value when it suffered a major data breach[22].

A comprehensive BCDR plan, therefore, must account for cyber risks and include policies for effectively navigating cyber events and – more importantly – preventing them.

[18] State of Cybersecurity Resilience 2021. Accenture. Retrieved August 15, 2022.

[19] Many security executives say they're unprepared for the threats that lie ahead. TechRepublic. Retrieved August 15, 2022.

[20] Businesses Suffered 50% More Cyberattack Attempts per Week in 2021. DarkReading. Retrieved August 15, 2022.

[21] Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025. Statista. Retrieved August 15, 2022.

[22] 250,000 People Leave Telco TalkTalk After Hack in October 2015. Business Insider. Retrieved August 15, 2022.

Disaster Recovery: Minimizing Downtime Due to a Cyber-Security Event_

Disaster recovery planning begins with risk mapping and impact analysis. Your goal is to identify two main metrics from all business systems:

- **Recovery time objective (RTO)** – maximum acceptable downtime for your application.
- **Recovery point objective (RPO)** – maximum period during which data can be lost from your application.

For example, for a payment processor, an RPO of several minutes can lead to significant compliance issues. In contrast, an RPO of several hours can be fine for some archival databases.

Based on the above metrics, you should design an optimal data backup strategy for different systems. As discussed earlier, this means implementing cloud backups of different services and data. Then implement suitable service failover mechanisms to secondary sites. Secondary sites should be equally secured and pen-tested as your main sites as intruders can detect them and take a secondary attack vector. Ensure that consistent security policies are applied to all sites by creating reference templates and testing against them.

Larger companies will also want to achieve geo-redundancy (i.e., create secondary sites in different regions to safeguard against local catastrophic events). Then, routinely verify your backup plan execution. Ensure that all backups are done as planned, are in a usable state, fully secured, and ready for failover.

Your next step is introducing smart process automation. When a cyber incident happens, a rapid response is required. Yet, everything appears to be a priority and your people need to act fast, leaving room for mistakes. To minimize errors and delays, introduce a degree of automation into DR workflows with solutions such as Azure Site Recovery.

Business Continuity: Ensuring Uninterrupted Business Operations_

Once the infrastructure has been redeployed (or protected) from cyberattacks, your next objective is to ensure business continuity.

If the previous set of actions were “recovery-centered”, business continuity planning focuses more on prevention. In this sense, BCP is strongly linked to overall cybersecurity excellence at your company. After all, you cannot maintain normal operations if your corporate systems were tampered with, data – malformed, or confidential information – exposed to unauthorized third parties.

Therefore, as part of BCDR, we always assess our clients’ current security posture and suggest additional cybersecurity solutions to cover existing gaps in identity management, access controls, asset protection, threat monitoring, and threat mitigation.

In the context of BCP, you should have the necessary solutions for minimizing (or fully eliminating) the impact of common cybersecurity events on your operations. This includes protecting your apps against frequent DDoS attacks. For reference, the volume of HTTP-layer DDoS attacks increased by 164% YoY[23].

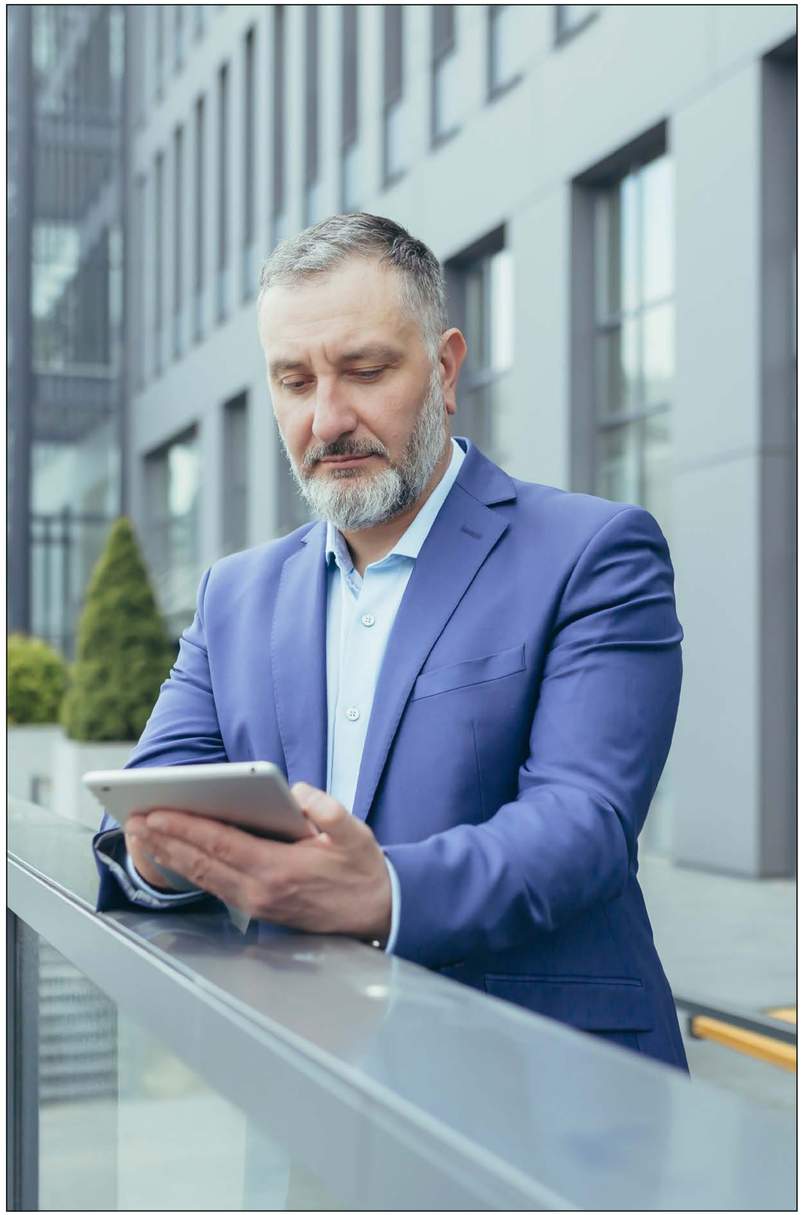
> Here you can find detailed Microsoft cybersecurity reference architecture – one of the approaches we base our recommendations on.

Likewise, to minimize the risks of unauthorized access and data leakage, you should implement proper user identity protection mechanisms and email security solutions. Azure AD and Microsoft Defender for Office 365 are the two tools for this task. Both of these tools help prevent risks associated with stolen credentials, malware distribution, and phishing attacks.

On an infrastructure level, you should deploy optimal firewall configurations to protect your web app against common cyber-attacks such as SQL injections, cross-site scripting, and local file inclusion among others. Azure Web Application Firewall (WAF) is a robust, cloud-native solution we recommend for this purpose.

Finally, focus on extended endpoint protection. Create a consolidated process for collecting security telemetry from various business tools and translating raw data into threat intelligence. Your goal is to progressively “connect the dots” between different systems and environments — networks, cloud workloads, on-premises services, email, business apps, and more — to understand where risks and vulnerabilities may emerge and to detect them fast. Cloud SIEM and SOAR tools such as Azure Sentinel provide your security teams with the coverage, scalability, and automation opportunities they may need.

[23] DDoS Attack Trends for 2022 Q1.Cloudflare. Retrieved August 15th.



Cybersecurity Questionnaire for BCDR_

When striving to create a viable BCDR solution, it is easy to omit some aspects that later turn out to be essential. To help you cover each and every element of the security design, we created this questionnaire that proves helpful at any stage of your BCDR journey.

1. How does your infrastructure ensure the high availability of services?
2. How do you conduct the backup process? What is the backup plan? How do you ensure consistency? For what period can data be lost? Does your backup plan satisfy those requirements?
3. How do you control that backups are made in time, not failing?
4. How do you run your backup/secondary locations?
5. Are there any differences in solutions, performance, or models?
6. How do you distribute configurations between locations?
7. How do you test the security of the same services in different locations?
8. Is your security team capable of monitoring main and secondary/backup locations with the same level of visibility?
9. Do your detection systems cover all sites and discover threats on secondary/backup locations?
10. How do you protect/isolate your backup system/ solution?
11. How do you isolate your management planes from main networks?

infopulse

Implementing BCDR with Infopulse_

Embed resilience into your corporate DNA with Infopulse technology advisory and security assessment services. Our consultants can conduct an in-depth audit of your current systems, map the risk radar, and cross-correlate various risks impact on different business systems, workflows, and operations in general. With a strong focus on security, our team helps SMBs and multinational companies alike implement robust disaster recovery and disaster mitigation controls to maintain continuous operations through any conditions.

Learn more about our technology & security advisory services.

About Infopulse

Infopulse, part of the leading Nordic digital services company Tietoevry, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & IT Operations, and Cybersecurity to SMEs and Fortune 100 companies across the globe. Founded in 1991, the company has a team of over 2,300 professionals and is represented in 7 countries across Europe and the Americas.

Infopulse is trusted by many established brands, such as BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Offshore Norge, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group, and others.

For more information, please visit **www.infopulse.com**

Contact us

PL +48 (663) 248-737

DE +49 (69) 505-060-4719

US +1 (888) 339-75-56

UK +44 (8455) 280-080

UA +38 (044) 585-25-00

BG +359 (876) 92-30-90

BR +55 (21) 99298-3389

info@infopulse.com