Honeywell | VEEAM

DISASTER RECOVERY AS A SERVICE FOR BUILDINGS OPERATIONAL TECHNOLOGY

A guide for the **CRITICAL INFRASTRUCTURE SECTOR**

Data Protection Technical Resource Guide

May 2023

CONTENTS

EXECUTIVE SUMMARY

Data is the lifeblood of every business.

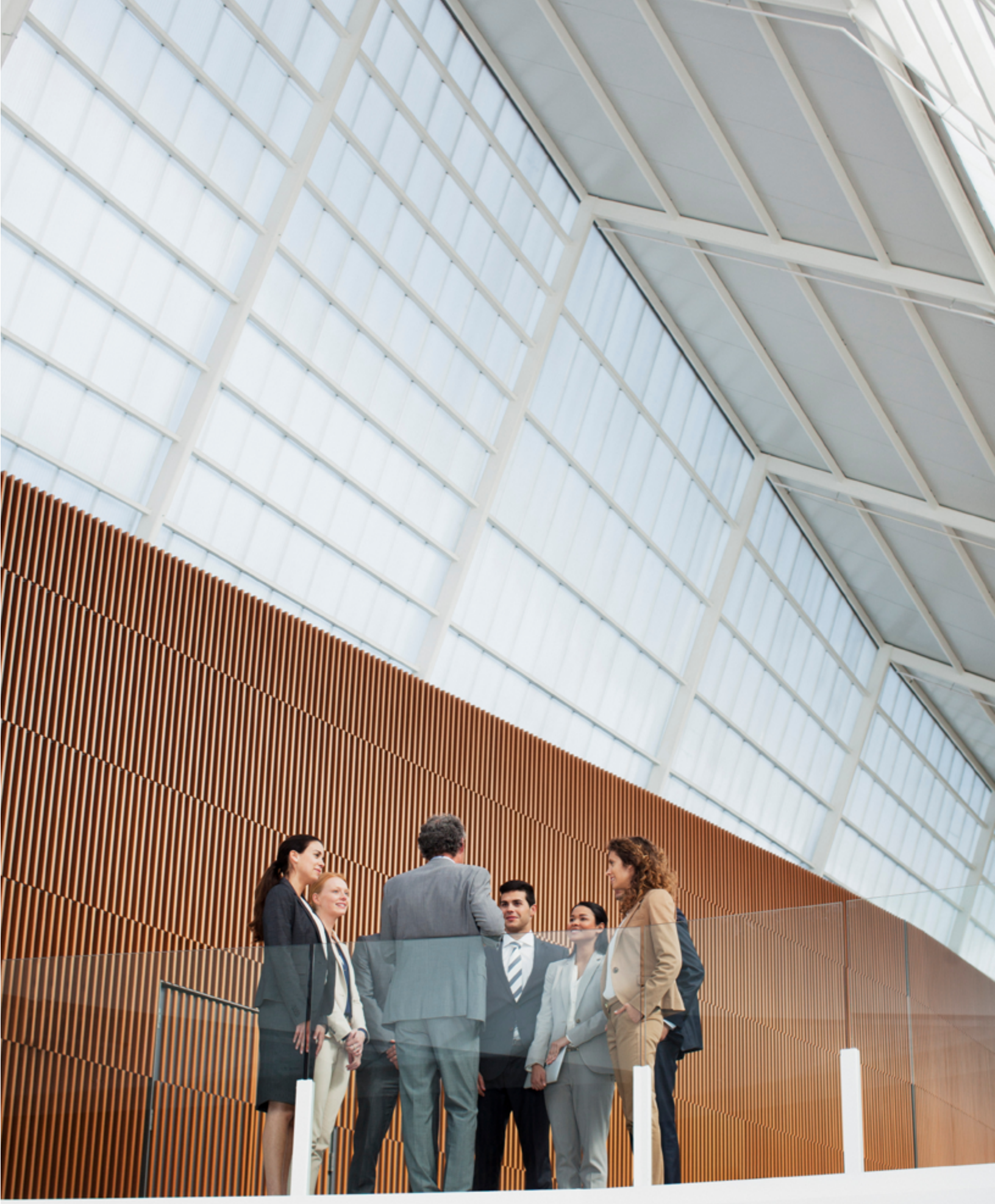
Any potential risk to business data needs to be mitigated with data protection. That's why Disaster Recovery (DR) solutions are important to the continuity of businesses today.

Many organizations, especially in the Critical Infrastructure (CI) sector, have prepared and implemented Business Continuity Plans (BCPs) including disaster recovery strategies to prepare for possible disasters, ranging from malware, earthquakes and floods to equipment failure.

While investing in DR is a smarter choice than risking significant downtime, oftentimes your IT team does not have the bandwidth or capability to plan, implement and manage this strategy. The good news is that more efficient options exist.

Disaster Recovery as a Service (DRaaS) offers a more manageable solution that offloads the end-to-end DR strategy from your IT department to a solution delivered "as a Service" by a credible partner.

DRaaS solutions also include coverage for your building's OT environments. This paper is designed to be your guide to what DRaaS is and why you need to implement it in your building's OT environment. We'll start by familiarizing you with the basic terminology, then we'll highlight the importance of DR solutions for CI organizations, how they work, and how DRaaS differs from traditional DR.



DEFINING KEY CONCEPTS

Let's first define the concepts that will underpin the content of this resource guide.

OPERATIONAL TECHNOLOGY (OT)

Operational Technology (OT) comprises programmable devices or systems that either manage devices that interact with a building's physical environment or interact with it indirectly.

OT systems continuously monitor and actuate processes, equipment and operational environments. Some examples include:

- HVAC systems
- Fire and life safety systems
- Building management systems
- Physical access control mechanisms

CRITICAL INFRASTRUCTURE (CI)

The Critical Infrastructure (CI) sector refers to organizations whose assets, systems and networks – physical or virtual – are vital to a country's economy, government or defense. The CI sector supports universally important services like communications, transportation, energy and water. Any disruptions or downtime to organizations within the sector could have potentially catastrophic consequences related to public health, safety or physical and economic security. Individual countries may define CI differently based on their infrastructure maturity.

BUSINESS CONTINUITY PLANS (BCP)

A business continuity plan (BCP) is a broad strategy that outlines how a business will keep running even in the event of a crisis situation. It focuses on a business as a whole, with different sections dealing with specific scenarios that could create operational risks. A BCP aims to keep critical operations running as close to normal as possible so that regular business activities can continue even during abnormal events.

DISASTER RECOVERY PLANS (DRP)

A disaster recovery plan is one of the different elements that make up a BCP. It is often focused specifically on the data and information systems of a business – in which case, it may be referred to as a data recovery plan. The simplest definition of this type of DRP is that it's designed to save, recover and restore data in line with the needs of an organisation in the event of a disaster.

These DRPs are usually developed to address the requirements of an IT department specifically, providing them with the tools, resources and processes they have to use to get systems and processes back up and running. With many businesses adopting digital workplace models, they are heavily reliant on their IT infrastructure for everyday operations . This is why DRPs make up a significant portion of BCPs.

WHY DO CI ORGANIZATIONS NEED DR?

Understanding why a CI organization needs a disaster recovery strategy is crucial in helping you identify potential risks.

Based on a recent report from Atlassian, the cost of downtime can range from $100,000 to $540,000 per hour[i] for medium- and large-sized businesses and enterprises. Businesses occasionally face many disruptions that require recovery. DRaaS solutions enable organizations to conduct routine validation testing to prevent business disruptions. They also provides redundancy for your critical information systems, which is why DRaaS is important for critical infrastructure organizations.

Furthermore, they can help maximize disaster recovery readiness by enabling a cost-effective and fast recovery process. It's like an insurance policy that provides disaster protection for your critical systems.

Below, we'll discuss the different types of disasters that have the potential to cause severe impacts to a CI organization.

1. CYBERATTACKS

Cyberattacks are on the rise, targeting businesses of all sizes globally. According to the Acronis Cyber Protection Week Global Report 2022, 36% of downtime events[II] were caused by cyberattacks. In a 2022 global study by the Ponemon Institute and IBM Security of 550 companies across 17 market sectors (from healthcare, education, industrial, to public government), 83% of organizations studied[III] were found to have more than one data breach.

Cyberattacks can come in several different forms, such as:

- Malware (for example ransomware)
- Phishing
- Password compromise
- SQL injection
- DNA tunnelling
- Zero-day exploits

OT systems are not immune. According to a 2020 Honeywell study[IV] of global facilities managers across four sectors, 27% had experienced a cyber breach of their OT systems in the previous 12 months.

Without a robust DR strategy, a single cyberattack could potentially encrypt or wipe away all of your data, wreaking havoc on your vital systems. In the Ponemon Institute/IBM Security study[V] the average time between a breach and breach detection was approximately 10 months. Think about the potential impact to your business of cybercriminals accessing your critical systems, undetected, for 10 months?

2. NATURAL DISASTERS

The increase in severe weather and weather-related natural disasters can also present a potential threat to OT systems.

Unfortunately, these types of disasters are often not preventable in the way that a cyberattack can be, so the focus needs to be on preparing business continuity plans that anticipate the impact and quickly deploying a disaster recovery plan to minimize impact.

3. TECHNOLOGY FAILURES

Technology failures can be particularly disruptive with on-premises data servers, causing extended downtime or permanent data loss. Poor implementation, lack of maintenance, misalignment and complexity are often among the most common causes of technology failure.

4. OT SPECIFIC ISSUES

In an Operational Technology (OT) environment, the effect of specific disasters can be magnified. Since the impact of a disaster in OT can be catastrophic, identifying and eliminating possible attack paths or failure points is essential. Operational systems by nature are objects and things we can see, feel or interact with in, such as elevators, security systems or access control systems. The impact of system downtime can impact staff, visitors or facility guests.

Risks may effect your business operations, controlled processes, equipment and even customers. Taking these factors into consideration when formulating a risk assessment approach in your DR strategy will help you identify the overall physical infrastructure your business operates within along with the associated gaps in operations and security.

HOW DO DISASTER RECOVERY SOLUTIONS WORK?

Here's an overview of how DR solutions work and what makes them different from BCPs (Business Continuity Plans).

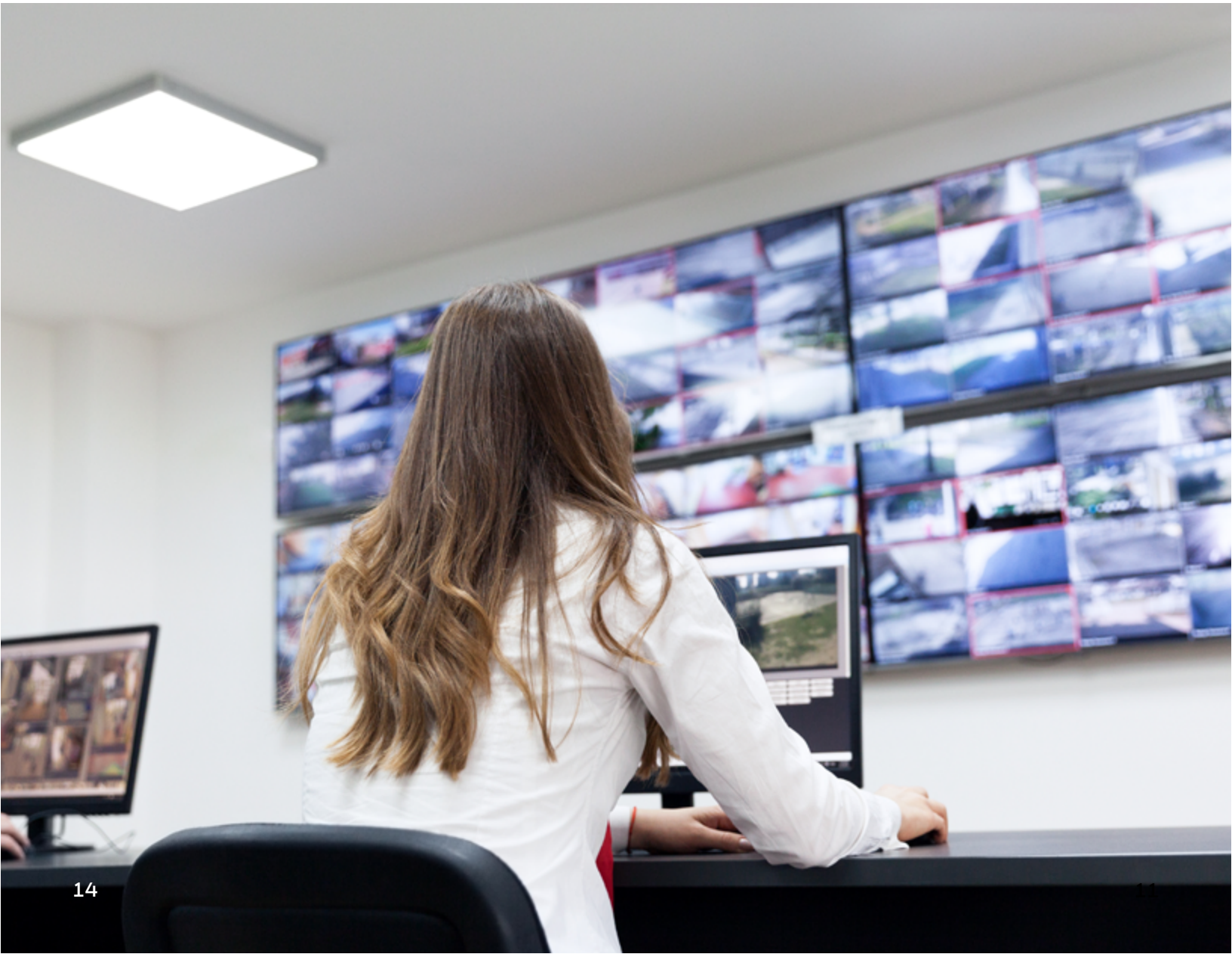
BCP VS DR KEY DIFFERENCES

CATEGORY	BUSINESS CONTINUITY	DISASTER RECOVERY
Purpose	Limits operational downtime	Limits abnormal or inefficient system functionality
Scope	Encompasses all the processes involved in safeguarding a company against all potential contingencies in a broad strategy	Focuses on the processes related to data access and IT
Timing	Enables a business to continue to provide services to customers with minimal disruption, whether during or immediately following a disaster	Focuses on the restoration of IT infrastructure and data access after a disaster has occurred
Focus	Keeps a business operating even in extreme circumstances and goes across all functions – technology, facilities management, HR, finance, customer services, etc.	Helps get business operations back to normal, for instance by addressing things like keeping network servers and OT systems working or recovering data

OVERVIEW OF DISASTER RECOVERY AS A SERVICE (DRaaS)

Disaster Recovery as a Service (DRaaS) is a cloud-based model that enables businesses to back up and recover their IT or OT infrastructure and data in case of disasters.

The main advantage of DRaaS is that your organization doesn't need to provision and administer the resources required for disaster recovery as they're offered and fully managed by the service provider.



KEY TERMS – DR/DRAAS

Familiarizing yourself with DR terminology will make it easier for you to understand how DR solutions can help your CI organization. The most important terms include:

Application Recovery
Comprises restoring business data and software once the operating system is restored and fully functional.

Failover
Protects computer systems from disruption by enabling the automatic takeover by standby equipment when the primary system fails.

Recovery Time Objective (RTO)
Specificies the period within which an organization must restore its processes after a disaster to keep the losses under control. It spans from the moment the disaster happens until the processes are restored.

Redundancy
Uses various sources or connections to guarantee that a single point of failure can't stop information flow.

Secondary Site
Provides a secondary place is where information is replicated from the production site, and acts as a backup in case that site is down.

Business Impact Analysis (BIA)
Predicts the extent of a disruption and its impact to business operations for the purpose of setting a suitable recovery strategy.

Production Site
Defined as the location where the original data resides.

Recovery Point Objective (RPO)
Identifies the maximum amount of data, as measured by time, within which an organization must recover data lost in a disaster. The RPO is defined by what the organization has estimated to be an "acceptable loss." It also determines the ideal replication method for each method.

Risk Assessment
Identifies possible business threats and disruptions, ranked by impact and chance of occurrence.

BENEFITS OF DRaaS FOR CI ORGANIZATIONS

These are some of the advantages of integrating a DRaaS solution into your CI organization:

ELIMINATE RANSOMWARE

Based on recent data from the Ponemon Institute and IBM Security[VI], ransomware can cost businesses US$4.54 million on average (not including the ransom itself), making it a risk that can't be ignored.

Ransomware encrypts an organization's data and demands a ransom in exchange for removing the encryption and releasing the data. Not only will a business have to pay a hefty ransom but it also runs the risk of continuing to lose money for as long as services are unavailable.

By implementing a DRaaS solution, you can better safeguard your CI organization's vital data by creating isolated but recoverable backups unaffected by the ransomware to keep processes running optimally.

PROTECT A RANGE OF WORKLOADS – INCLUDING OT

As reported in the Honeywell study[VII], only 44% of respondents had a cybersecurity system in place for their OT systems, meaning more than half of OT systems had no specific cyber threat protection in place.

DRaaS solutions enable you to protect any workload you want, including operational technology workloads. Regardless of the complexity of your business workloads or operations, protection is guaranteed across all your OT workloads.

ADVANTAGES OF DRaaS VS. TRADITIONAL DR

Both DRaaS and traditional DR have the same objective: quickly recovering systems after a disaster. There are substantial differences between the two approaches.

AUTOMATION AND MANAGEMENT

DRaaS solutions enable you to create and manage recovery plans with a unified environment for production and DR sites. You can also implement automated DR orchestration in all your virtual machines.

DRaaS solutions also let you use a consistent operating experience with automatic failover and failback for both on-premises and cloud systems.

Adopting a DRaaS solution also means less worry about life cycle management thanks to automatic updates that eliminate the need for renewals or other manual tasks.

As a SaaS-based model, DRaaS solutions remove the complexities that are often associated with disaster recovery strategies. Compared to traditional DR systems, there are no maintenance or operational tasks to hog your IT resources; everything is managed by the service provider.

ADVANTAGES OF DRaaS VS. TRADITIONAL DR (continued)

SCALABLE

One of the most significant advantages of DRaaS over traditional DR is scalability. DRaaS solutions can be scaled up or back seamlessly as your data backup and recovery requirements change. Being built on a virtual platform, you can grow or shrink your DRaaS data stores on demand.

Since traditional DR requires a huge investment to set up and manage, attempting to scale it up or down can be costly and time consuming. Not to mention, a DRaaS solution keeps data in discrete locations, eliminating the "single point of failure."

FLEXIBLE FAILOVER AND FAILBACK

DRaaS is quite flexible. There's no server lock and you can use the backup technology, database, operating system and management systems best suited for your organization with no restrictions.

DRaaS also lets you choose the recovery destinations for a partial or full recovery. You can even restore individual files. Many DRaaS services also enable you to use resources on demand based on your organization's requirements.

Traditional DR, on the other hand, means you're locked to one server, and the choices of operating systems and backup technology are limited. Moreover, DRaaS offers the ultimate flexibility in terms of deployment options. also
It also has the ability to set up failover capacity with a minimal footprint or 100% on-demand.

REPLICATION ADVANTAGE

DRaaS lets you replicate your CI organization's backup data to a third-party service provider or public cloud infrastructure, allowing for fast recovery with low recovery time and recovery point objectives (RTOs/RPOs).

Additionally, it removes the need to invest in a second data center infrastructure for the purpose of disaster recovery, helping to reduce costs.

With traditional DR, you have to operate a separate off-site data center for recovery, and the recovery time will be considerably longer than with DRaaS.

PROTECTING CRITICAL INFRASTRUCTURE FROM DISASTERS

The very nature of critical infrastructure means that it's failure can cause serious issues, and therefore threat actors are drawn to critical infrastructure as a way to destabilise cities, industries or even whole countries.

A part of any business continuity plan for CI must include a Disaster Recovery component that will enable critical data, systems and processes to be recovered quickly and seamlessly in the instance that the worst occurs.

Honeywell's commitment is to not only ensure buildings run well, but also that their systems have the resilience to maintain and ensure provision of services under a wide range of conditions.

To achieve this, Honeywell provides a comprehensive OT DRaaS solution that provides a consistent user experience, boosts efficiency and maximizes service availability for key building technologies.

The implementation of a DRaaS solution allows critical infrastructure operators to guard against ransomware, protect a range of workloads – including OT – and gain the control to manage RTO/RPO settings in line with business needs.

That's how we can make resilience a key attribute of critical infrastructure.

READY TO PROTECT THE OT OF YOUR CI ORGANIZATION?

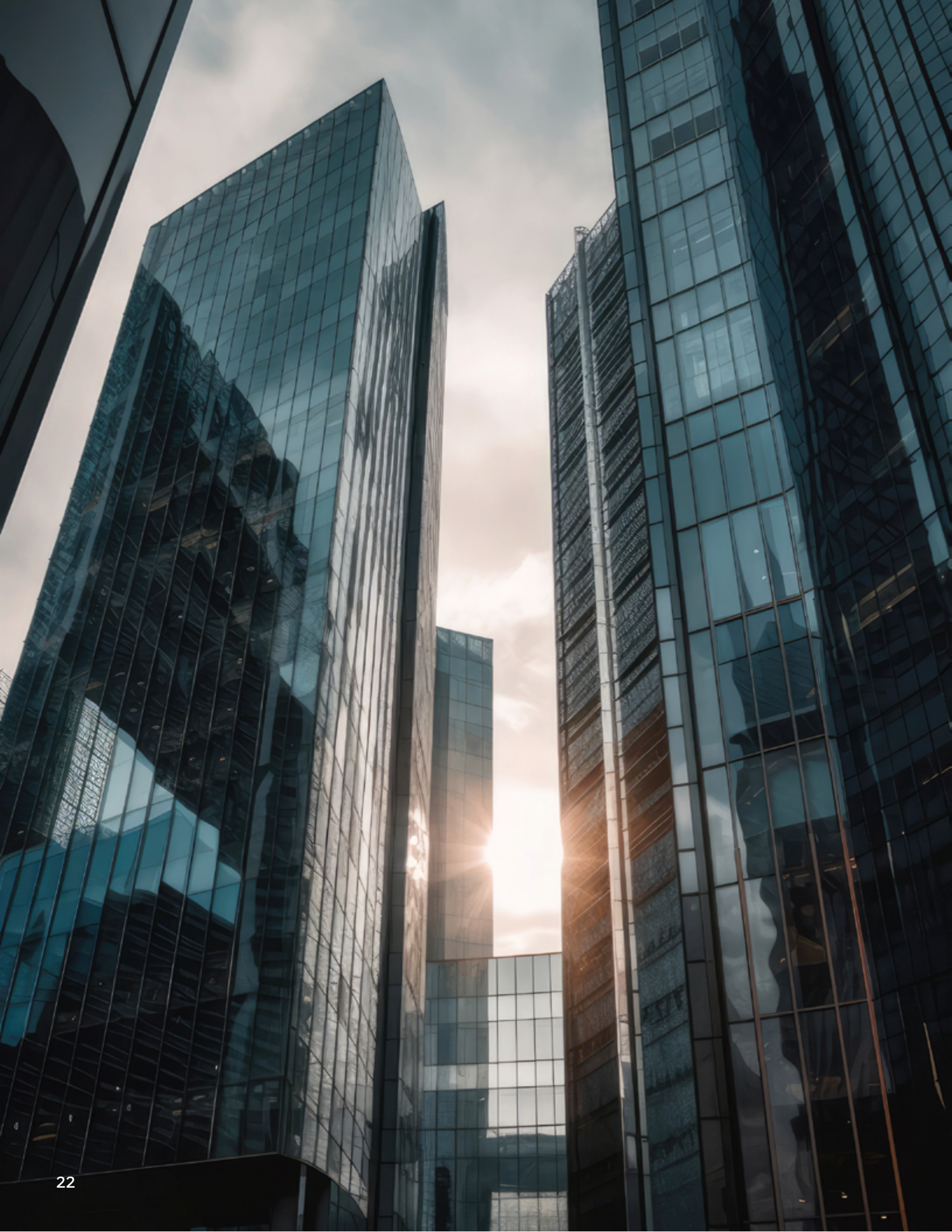
Contact your local Honeywell Buildings representative to schedule a site assessment and help you formulate an business continuity plan that includes a disaster recovery approach to meets your needs.

Honeywell Cybersecurity website

https://hwll.co/HoneywellCybersecuritySolutions

Contact Honeywell Cybersecurity

https://buildings.honeywell.com/us/en/support/contact-sales



REFERENCES

[I] Atlassian, "Calculating the cost of downtime". [Accessed November 20, 2022]

[II] Global NewsWire, "76% of organizations suffered downtime and data loss in 2021, system crashes, human error and cyberattacks to blame", Acronis Inc., March 31, 2022. [Accessed November 20, 2022]

[III] IBM, "Cost of a Data Breach Report 2022", Ponemon Institute and IBM Security, July 2022: [Accessed January 23, 2023]

[IV] Honeywell, "Honeywell Survey: 71% Of Surveyed Facility Managers State Concerns About Operational Cybersecurity", Honeywell 2021 Building Trends Series, August 25, 2021. [Accessed January 23, 2023]

[V] IBM, "Cost of a Data Breach Report 2022", Ponemon Institute and IBM Security, July 2022: [Accessed January 23, 2023]

[VI] IBM, "Cost of a Data Breach Report 2022", Ponemon Institute and IBM Security, July 2022: [Accessed January 23, 2023]

[VII] Honeywell, "Honeywell Survey: 71% Of Surveyed Facility Managers State Concerns About Operational Cybersecurity", Honeywell 2021 Building Trends Series, August 25, 2021. [Accessed January 23, 2023]

For more information
www.BuildingSolutions.Honeywell.com

Honeywell Building Technologies
1985 Douglas Drive North Golden Valley, MN 55422-3992 Tel:
1-800-345-6770 www.Honeywell.com

Data Protection Whitepaper | 05/23