OTAVA®

SECURE & COMPLIANT MULTI-CLOUD SOLUTIONS

IT Disaster Recovery Plan: Don't Wait for Chaos to Hit

Proactive Steps to Safeguard Your Business and Ensure Rapid Recovery

As organizations rely on data to advance every facet of their business today, ensuring rapid recovery in moments of unexpected chaos or natural disasters is essential to avoiding costly disruptions or data loss. Cloud-based disaster recovery as a service (DRaaS) offers immediate business continuity, minimizes downtime and provides continuous protection through always-on encryption and scalable, purpose-built solutions that can be deployed anytime, anywhere. Gartner recently noted that "72 percent of organizations are poorly positioned in terms of disaster recovery capabilities, with 63 percent likely suffering from 'mirages of overconfidence.'" That means that when disasters strike — hurricanes, power loss or service outages, cyber-attacks or worse — downtime equates to loss of data, impacts to the bottom line, regulatory consequences and loss of customer or consumer confidence.

- **Get Back Up and Running, Immediately:** The importance of rapid restoration of critical business functions following an incident cannot be overstated. Learn how cloud-based solutions help teams restore faster.
- **Recover, Isolate and Restore:** Understand the S.E.C.U.R.E.™ Framework's "Undo" and "Recover" pillars and the proactive steps businesses can take to isolate and restore infected data and get back up and running.
- **Take a Wholistic Approach to Managing Risk:** Craft an incident response plan that spells out goals, procedures, inventory and communication needs, and integrates DRaaS.
- **Maintain Continuity and Compliance:** Reduce risks of regulatory fines or penalties resulting from cyberattacks, natural disasters, human error or negligence by putting proactive measures in place.

How We Got Here: The Latest Trends in Security and Recovery

Business and IT leaders frequently discuss the concept of cyber resilience, but what does it truly mean for an organization to be cyber resilient? Beyond ensuring cybersecurity protections against external threats, cyber resilience encompasses risk mitigation and response, proactive planning for attacks, natural disasters and human errors (or negligence), and prescriptive steps for recovery following those events. Understanding that risks cannot be avoided, achieving true cyber resilience allows leaders to ensure everyone knows what to do, understands which data and IT are essential, and prioritizes restoration and recovery of key assets to maintain continuity and lessen business interruptions.

Contents

As organizations battle new forms of AI-generated ransomware threats, deploy increasingly complex, cloud-dependent environments, and empower remote teams (and more) through edge computing, achieving cyber resilience becomes not only more complicated, but also more critical.

Ransomware Evolves

Gartner's 2024 report "How to Prepare for Ransomware Attacks" warns that bad actors continue to change tactics as their older tried and true methods are increasingly thwarted. "Extortionware," or data-stealing ransomware, is an encryption-free data theft attack, and only one of the latest string of ransomware tactics gaining speed. Double extortion involves encrypting stolen data and threatening to leak it if an organization refuses to pay the ransom. Bad actors also mine stolen data to identify other potential sources of revenue: So-called "triple extortion" demands ransoms, in turn, from a victim organization's partners or customers. "Phishing, remote attacks on public-facing infrastructure and authorized remote desktop connections continue to be the primary sources of infiltration for ransomware," the report states, adding that the cost of recovery and resulting downtime, as well as the cost of the reputational damage to the organizations that suffer those breaches, "can amount to 10 times the amount of the ransom itself."

$5.2 million

The average extortion demand per ransomware attack in the first half of 2024

Source: Comparitech

Multi-Cloud Environments and Edge Computing

Organizations increasingly rely on multiple cloud providers for everything from cloud-based infrastructure and storage to applications and threat monitoring, and much more. These multi-cloud environments enable organizations to deploy essential IT in more cost-effective and efficient ways than single-provider or exclusively on-premises environments. The rise of the multi-cloud approach has also prompted a rapid rise in edge computing, where data processing and compute happens locally — at the edge — reducing latency and improving UX for remote workers and consumers alike. In many ways, the rise of edge computing devices and applications drove the rise of multi-cloud strategies, but this chicken-or-egg question is not as important for organizational leaders to resolve as is the need for understanding how data loss prevention, backup and recovery strategies must evolve as a result of this modern, rapidly shifting IT landscape.

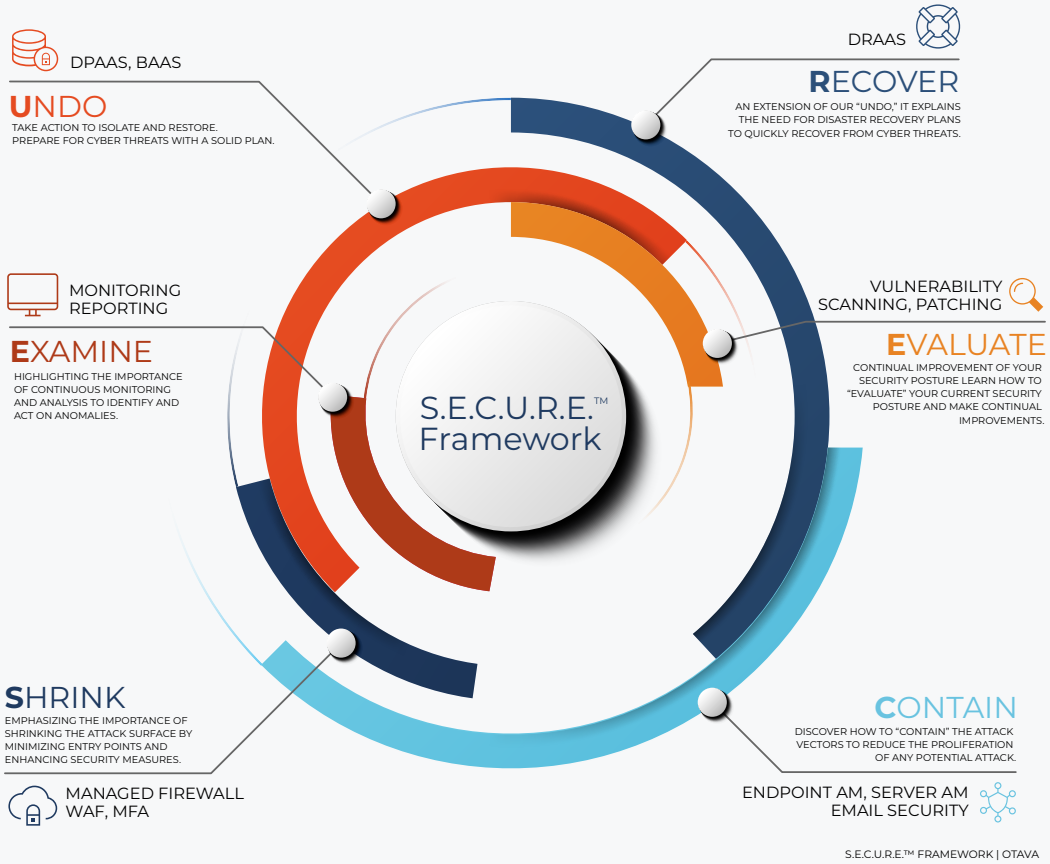
Why Choose DRaaS?

Such distributed data and computing environments significantly increase the attack surface, requiring new thinking around access and security policies that account for the many diverse platforms or applications an organization leverages through the cloud. Yet that same distribution across multiple cloud providers also provides some level of built-in redundancy, enabling more seamless failover in case of a provider outage, and more effective means of disaster recovery.

Businesses and other organizations have by and large turned away from on-premises disaster recovery solutions for several reasons, not least of which is the time and cost associated with restoring data or environments from physical media like tape. Given the exponential growth of data across all areas of business and industry, relying on physical media to restore all that information rapidly, without interruptions to business or significant impact on the bottom line, simply is no longer sustainable. Cloud-native disaster recovery solutions, instead, offer scalable backup and recovery protections that meet the growing complexity of today's multi-cloud, data-rich IT environments.

The S.E.C.U.R.E.™ Framework — What Does It Stand For?

- **Shrink:** the **attack surface** and protect access points
- **Examine:** **monitor and analyze** anomalies and event threats
- **Contain:** the **attack vectors** to reduce the proliferation of any attack
- **Undo:** take action to **isolate and restore** infected data
- **Recover:** to achieve **business continuity** of operations
- **Evaluate:** continual improvement of your **security posture**



S.E.C.U.R.E.™ FRAMEWORK | OTAVA

Security resilience is a journey, not a one-time task. It demands ongoing updates and refinements to safeguard systems, networks, and programs from digital threats. OTAVA's S.E.C.U.R.E.™ Framework is designed to meet businesses at any stage of their cybersecurity journey, providing a strategic approach to business continuity through layered prevention, visibility, contingency planning, and continuous improvement.

Time is of the Essence

What factors influence recovery success following an incident? What's required for rapid restoration? Before understanding how to recover rapidly, it's important to understand how recovery success should be measured. Two primary metrics gauge recovery success or failure:

Recovery point objectives (RPO), represent the maximum amount of data loss an organization can withstand following an event. This metric is expressed as time, typically the time between the most recent backup and the event.

Recovery time objectives (RTO), represent the amount of time an organization is willing to allow for full restoration of its critical infrastructure, data and processes to pre-event service levels following a threat or other downtime. This metric is typically defined to ensure minimal interruptions to customers or business processes.

It's important for organizational and IT leaders to understand how to establish specific and realistic goals for each, and what affects them. There are many factors to consider:

The S.E.C.U.R.E.™ Framework, built on the NIST Cybersecurity Framework, helps teams manage cybersecurity risks across industries by:

- **Identify Gaps**
- **Improve Compliance**
- **Promote Stakeholder Collaboration**

- How important is this data or asset to the organization? A healthcare organization, for example, most likely cannot wait more than an hour or two to restore critical services if they would impact patient health.
- What are the associated costs? The more stringent the RPO and RTO goals, the more expensive they may be to achieve. Beyond costs associated with losses, also consider the costs of transferring data, storage, and other recovery costs. This is just one area where DRaaS adds greater value.
- What are the associated risks? Does everyone understand how critical each system or data element/category is to the organization? Can they be ranked or prioritized to determine or otherwise show how their loss will affect the organization's overall health or success? In most cases, a risk assessment and business impact analysis should be performed.
- Have you heard from everyone? Seek stakeholder input before finalizing RTO and RPO goals, to ensure nothing critical is left behind or misunderstood.

Depending on the industry or business type, leaders may also need to consider their contractual or service obligations to customers to restore data and other essentials within a set time and/or maintain specific RTOs/RPOs.

"Reflect on your current readiness," advises Chris Barylski, Product Manager at OTAVA. "Knowing where to start with DR services layered on top of backups and how to recover promptly is critical."

What's the Plan?

A comprehensive incident response (IR) plan or disaster recovery plan (DRP) details not only RTOs and RPOs but also goals, required backup and DR procedures, restoration processes, inventories and communication essentials that everyone in an organization must follow whenever disaster or threats strike. While the IT organization typically writes an IT DRP to address hardware and software restoration priorities, organizations also should craft and follow a broader business continuity plan that addresses essential data, backup and recovery, and more. Organizations without an up-to-date IR or business continuity plan or playbook should ensure a newer version addresses those key areas, alongside any industry-specific requirements that also must be taken into account in the event of an outage or downtime. While the process may seem daunting given all that IT and other C-suite leaders must focus on day in and day out, the task cannot be put aside.

NIST offers several resources and frameworks for teams to consult for help.

What's at Stake?

Disaster recovery planning, and DR solutions more specifically, are critical to isolating and restoring affected data and infrastructure, and minimizing losses when disaster strikes; tests are essential for understanding whether the intended plan and solutions will actually work in the moment of emergency. Periodic and regular testing highlight gaps in planning and protections as well as areas where recovery can improve, or when additional backups may be required.

Disaster recovery testing specifically tests an organization's DR plan and shows how well (or whether) an organization's critical systems and data will be recovered. DR testing shows how well an organization is equipped to meet RTOs/RPOs, and the adjustments that can improve those objectives.

Backup and recovery testing shows whether data has been backed up completely and consistently and whether it is accessible in the event of a loss.

Several industries must show that their DR preparation and planning also comply with regulations because they are required by law to ensure robust systems are in place to recovery data and information quickly in the event of disruption.

Finance

Financial industries are beholden to oversight groups like the FDIC, which requires comprehensive DR plans and regular testing to ensure business continuity and more. A well-developed plan helps to build and maintain consumer trust. Testing also helps organizations identify vulnerabilities and proactively address associated risks. Financial organizations must maintain detailed plan documentation and often must engage third-party auditors to perform required tests.

Healthcare

HIPAA mandates robust data protection and system availability, even during disruptions to service within healthcare organizations. That requires regular testing and documentation of DR plans, like finance, to prove their ability to recover patient information in the event of a disaster, disruption or breach. Some regulatory bodies within the sector may conduct audits to assess an organization's capabilities and response procedures. The potential for stiff fines and legal penalties for organizations that fail to protect patient data or adhere to HIPAA guidelines is high and, at worst, compromises patient care and safety.

Manufacturing

Similar to healthcare and finance, many manufacturers answer to oversight bodies that require well-documented DR plans, regular testing, audits and verification of compliance with relevant industry or sector standards. DR plans must account for data and IT service interruptions as well as OT — operational technology — interruptions. OT covers industrial equipment and related networks, SCADA or controllers, which are more frequently targeted by nation-states and other threat actors due to their high vulnerability. Disasters and prolonged recovery in these environments can harm employee safety or public health in addition to the manufacturer's bottom line.

What Could Go Wrong?

Data and IT losses commonly result from natural disasters (hurricanes, floods, earthquakes), service outages (power or cloud partner/provider), cyber threats and other inevitable threats — the list is as great as your imagination and capacity for worrying about the worst-case scenario.

Planning and preparing for the worst, using global best practices and regulatory guidelines ensures the fallout from those scenarios can be minimized. Cloud-based DRaaS offers another layer of protection, through on-demand service and purpose-built solutions, ensuring faster recovery and improved resiliency while proactively preserving business continuity, whenever and wherever disaster strikes.

Key Considerations

- When was your recovery plan last updated?
- What would a loss today cost your business or organization?
- What disaster recovery processes and solutions are now in place?
- Is your organization compliant with current regulatory requirements for data protection and loss?
- Have any of those regulations recently updated, requiring changes or updates to your plan?

Streamline Your Disaster Recovery Plan with OTAVA

OTAVA's fully managed Disaster Recovery as a Service offers the rapid recovery of data and virtualized applications that today's businesses demand. Deploy in any location at any time and conduct tests as often as needed. Rest easy knowing your data is always encrypted, both in transit and at rest, keeping your confidential information safe and secure.

Learn More

OTAVA solves modern, critical challenges for their customers via sophisticated secure and compliant multi-cloud solutions aligned with industry standards and people-centered, best-in-class professional services built on the foundation of collaborative relationships.

When it comes to implementing cloud solutions, OTAVA knows one size doesn't fit all, so its team of IT professionals will help you along your journey to migrate and integrate your cloud solutions in adherence to the S.E.C.U.R.E.™ Framework.

Contact an OTAVA expert today to learn more by visiting otava.com.

Take a security assessment today and learn how OTAVA will secure your operations against cyber disruptions.

OTAVA

SECURE & COMPLIANT MULTI-CLOUD SOLUTIONS