Annual International Scientific Conference
"Competitiveness and Innovation in the Knowledge Economy"
September 26-27, 2025
Chisinau, Republic of Moldova

DOI: https://doi.org/10.24818/cike2025.62

BACKUP AND RECOVERY STRATEGIES IN MODERN ENTERPRISE IT SYSTEMS

ZGUREANU AURELIU
PhD, Associate Professor
Academy of Economic Studies of Moldova,
Chisinau, Republic of Moldova
e-mail: zgureanu.aureliu@ase.md
ORCID ID: 0000-0003-3301-2457

ANDRONATIEV VICTOR
PhD, Associate Professor
Academy of Economic Studies of Moldova,
Chisinau, Republic of Moldova
e-mail: andronatiev@ase.md
ORCID ID: 0000-0002-0294-457X

Email addresses of corresponding author: zgureanu.aureliu@ase.md

Abstract: Assessing the current state of enterprise backup and recovery strategies is critical to ensuring that an organization's digital assets are safeguarded against a variety of internal and external threats: hardware and system failures, human errors, malicious cyberattacks such as ransomware, etc. This paper examines the evolution of data protection from traditional, reactive approaches to comprehensive, proactive resilience frameworks. The paper provides a breakdown between the foundational data protection strategies of on-premise, cloud and hybrid methods of data protection and restoration with explanations of the pros and cons of each method from the perspectives of control, scalability and disaster recovery. The analysis extends to advanced methodologies such as Disaster Recovery as a Service, Continuous Data Protection for recovery at the most granular level, and to the importance of immutable storage to avoid data alteration. Paper analyses today's challenges of voracious data growth, new types of data residing in increasingly fragmented environments, and the ever-evolving sophistication of malicious actors especially as it relates to ransomware targeting backup infrastructure. It also explores the use of emerging technologies, especially Artificial Intelligence and Machine Learning to conduct predictive analytics, detection of anomalies, and the automation of recovery with architectures such as air-gapped and chain-free backups to provide greater levels of isolation. Finally, the impact of global regulatory compliance standards (GDPR, HIPAA) on modern-day data protection is discussed and relevant industry standards (NIST, ISO 27001) that have become best practices are reviewed.
Keywords: Data protection strategy, DRP, DRaaS, CDP, RTO, RPO
JEL Classification: L86, M15

1 Introduction

Today's enterprise backup and recovery goes far beyond daily operations, regarded as a key "digital insurance policy" for an organization's data assets. This represents a complete evolution from a reactive to a proactive and multi-faceted risk management approach that is within organization's business continuity and operational resilience (Arcserve, 2025).

Today's backup solutions often implement a hybrid approach of on-premises, cloud, or a combination of both including arbitrary backup types including full, incremental, and snapshots. Data deduplication is an important factor for efficient use of storage and faster recovery, while solid encryption policies protect data at rest and in transit. The strategic imperative is seamless integration into overall disaster recovery (DR) plans and not only testing, but conducting drills on

a regularly scheduled, ongoing basis after the backups are put into normal operation. The end goal is to restore daily business operations as rapidly and as seamlessly as possible, against cyber-attacks such as ransomware that may encrypt or delete operational data. Effective data backups allow an organization to "transplant" their data to a newly restored, healthy version allowing them to continue business operations. Leading players for DR solutions, such as Google Cloud's Backup and DR Service offer competitive features such as backup vault protection, aggregate management system components, automated retention and recovery options - cross region/cross-project - and all with solid encryption (Google Cloud, 2024). Systems like Rubrik unify data security and protection through zero-trust data protection policies, malware investigation, orchestrated application recovery emphasizing the need to maintain a coherent view of so-called data resiliency.

The move from data copy to comprehensive "digital insurance", serves to reinforce the notion of data protection as a business function. This strategic shift is amplified by the focus on automation, integration, and rapid recovery, contrasting with traditional, often manual, methods. Sentiment towards rapid recovery and instant recovery, policy-based automations, and other steps to execute backups and recoveries note that today's backup and restore create and continue business only very briefly.

Enterprise-grade IT systems comprise an entire stack of hardware, software and services components that are provided specifically for the purposes of large organizations to better manage internal and external distributions of efficient and productive ways to conduct business. This ecosystem includes high-performance servers, diverse storage devices, robust networking equipment, and critical software applications like Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM). Enterprise IT solutions environments are always changing and evolving with business demands, where technology, cloud computing and Artificial Intelligence are the leading technology enablers.

Complexity and distributed environments of enterprise IT systems will redefine future backup and recovery needs, successfully transitioning from a centralized approach to data protection and cyber resiliency to embrace a distributed perspective. Such fragmentation will create enhanced data backup and recovery that is distributed, and integrated, and operate across many different locations and data management formats and shift the mindset from "backup copy" concepts to a holistic distributed and "resilience" ecosystem. Digital transformation, cyber-attacks and fast-growing data continues to reinforce the positioning of backups and recovery in organizations overall cybersecurity. The priority areas of the business continuity strategy are algorithms and metrics.

2 Foundational Backup and Recovery Strategies

Backup and recovery solutions are viable options, both on premise and in the cloud, which offer different pros and cons. These two methods can even be combined and adjusted to meet needs of different organizations and systems. The choice between on-premises solutions and cloud-based solutions is the first step in the decision-making process for modern enterprise backup strategies, with each providing unique technical merits, pros, and cons.

Cloud backup solutions send copies of an organization's data to remote storage systems, and is usually hosted, managed, and maintained by third-party providers that charge subscriptions fees based on storage, bandwidth, and users. Various pros of cloud-based backup solutions are better data protection from agency risk, such as malware, natural disasters, and human error exposure. Reliability is another benefit since the process is automatic and always 'on'. File recovery is highly simplified compared to on-premises methods and IT staff can spend less time on file recovery. Accessibility is significantly improved, allowing global retrieval with an internet connection, beneficial for mobile workforces. Rather than a fixed storage number or physical warehousing of the equipment, cloud storage methods are scalable in nature: they can 'grow' along with demand to an extent, and organizations pay for only what storage they utilize, not for excess storage space

when they don't need it. A new cloud vendor can provide an organization's storage need without requiring mass quantities of hardware, and installing. Financially, cloud-based solutions always have lower up-front setup fees and usually come with ongoing maintenance. Being outside of the organization site, cloud backups generally support quicker file recovery. Data security is addressed through encryption of data at rest and in transit, stringent security protocols, 24/7 monitoring, and compliance support (Dropbox, 2025).

In-house backup stores the organization's backup data on physical servers located at the business location. The biggest advantage of in-house backup is that the backup infrastructure is physically in control of the organization; therefore, the organization retains control of the data that is determined to be most critical, including all aspects of privacy - because the organization is storing all backup data physically at its location and does not have to worry about outside access. Another advantage is that there is no dependency on obtaining data from an internet connection, which is very important to organizations that cannot rely on a consistent internet connection or organizations that have strict low latency requirements. For some small to mid-sized companies, in-house backup solutions can be more cost-effective in the long run and can have the organization printing out proprietary procedures and documents on their own.

At the same time, on-premise solutions do require an upfront capital investment in storage hardware and supporting infrastructure that must be identified and purchased. Scalability is always a challenge for on-premises storage solutions, especially since increasing volumes of backups typically entail buying more hardware. It can also be complicated and resource-consuming to make sure independent compliance is met. Therefore, on-premises solutions usually have slower recovery time objectives (RTO) and less frequent recovery point objectives (RPO) than cloud solutions (Zgureanu, 2022).

Hybrid backup architectures are a sophisticated and growing trend in enterprise technology and attempts to use both on-site and cloud solutions to leverage the strengths of each while minimizing weaknesses. In this regard hybrid backup architecture, involves a centralized management system that allows for local and cloud backup operations to be consolidated and streamlined (Andrews, 2025).

One of the most significant benefits of hybrid solutions is the additional redundancy that they provide in disaster recovery. Having two copies of data available, one locally and the other in the cloud, gives organizations multiple layers of protection against various forms of data loss or system failures. The addition of redundancy is a vital component in maintaining business continuity. Additionally, hybrid architectures offer faster recovery times in two ways: businesses can typically recover critical and frequently accessed data quickly from local backups, which often have lower latency, while cloud backups can be relied upon for long term retention and recovery from major site-wide disasters.

Disaster Recovery as a Service (DRaaS) has emerged as one of the most significant service models in the cloud computing industry to date that gives an organization the ability to backup their data and IT infrastructure in a third-party cloud environment. However, a DRaaS provider is not just merely data storage; they have the capability of orchestrating and therefore can allow organizations to be able to quickly restore their IT infrastructure back to their operable state upon breaking event. As a DRaaS model is fundamentally an outsourcing model that takes the responsibility of provisioning and maintaining an organization own offsite Disaster Recovery environment and takes it on by a specialized service.

The main feature of DRaaS is that it is a mirror of IT infrastructure - an organization's computer, storage, and network functions are mirrored in a fail-safe mode in virtual servers. This means that an organization who has suffered a disaster can keep running applications from the service providers hybrid cloud or cloud infrastructure, designated for disaster recovery without interrupting resources on their own physical servers that were affected by the disaster. As a result,

we obtain a faster recovery time. DRaaS thus plays a key role in ensuring resilience, minimizing recovery time after a disruption that can significantly impact productivity, sales, customer service, and profitability. DRaaS provides recovery tools for various types of disruptions, such as natural disasters, equipment failures, power outages, and increasingly sophisticated cyberattacks.

Continuous Data Protection (CDP) is commonly referred to as continuous backup or real-time backup and is a highly sophisticated strategy that captures and stores data modifications as they occur. Unlike most traditional backup procedures, which are performed at set intervals, a DRaaS provider continuously (while the environment is active) records data about every change in real time (thus allowing the organization to restore data to any point in time); this is a key difference for this approach. However, this type of data recovery provides the enormous granularity achievable with a CDP and potentially near-zero data loss (assuming a zero RPO is achieved).

Continuous Data Protection works as it captures data in an enterprise system and backs-up the changes in files each time a file is changed, with essentially a copy of each changing aspect saved near real-time or very quickly, all in a separate data storage infrastructure. The automated data protection of CDP represents a huge efficiency gain in operational environments in regard to setting up protective measures around changes, since it removes humans from the safeguarding process related to changes. CDP is particularly crucial in environments where data is constantly changing and the cost of data loss is exceptionally high, such as in financial services, healthcare, and e-commerce platforms, where real-time transactional data is paramount. CDP is also very useful to prevent disasters as it provides the ability to recover from any point in time of prior to the disaster event happening in an operational environment, which also minimizes recovery time and data loss. The difference in CDP vs a snapshot-based backup is that CDP is continuously backing data up each time there is a change made to the data, in the sense that there haven't been any significant changes made during the period of backup.

Immutable storage is implemented under a Write Once, Read for Many (WORM) principle or governed by software defined storage. Based on policy rules configured by the administrator, once the data has been stored under the policy, the immutable data will be secured from modification, overwriting or deletion for the specified immutability period. The benefits of immutable storage for data protection purposes are substantial. It can provide data integrity and compliance, support business continuity plans, protect against human error, retard support incident response and defend against ransomware attacks.

However, immutable storage does have limitations. The very nature of the immutability will prevent modification, deletion of the stored data until the applicable retention period has expired meaning we need to do careful capacity planning to prevent unintentional budget increase for storage costs. Immutable storage will provide data integrity; however, immutability itself does not protect against total loss of data. It must go hand in hand with a backup and disaster recovery strategy. Management and implementation of an immutable storage solution may require specialist skills and human resources.

Immutable storage is becoming increasingly a non-negotiable component of data protection because of heightened ransomware sophistication and scrutiny (Cloudian, 2025; Arcserve, 2025). While offering unparalleled data integrity, the cost implications and management complexity necessitate a strategic approach to data classification and retention, ensuring only truly critical data is subjected to long-term immutability.

3 Addressing Key Challenges in Enterprise Data Protection

The exponential growth and increasing diversity of data is one of the biggest challenges facing modern-day enterprise data protection and Data Lifecycle Management (DLM). With an abundance of digital devices and platforms, organizations are collecting increasing volumes of data, from structured data in databases to unstructured data in text, images, and video. To say this

presents a storage challenge is an understatement. Organizations have begun investing in very scalable storage options to scale their data storage constraints without compromising performance. Additionally, processing and storing data in different formats often increases complexity and functionality, as multiple data types are often involved. It is a common occurrence that enterprises are now generating petabytes of data that would overwhelm file storage processes not built for these volumes. This challenge is magnified by the need for organizations to keep multiple backups in their data protection strategy, effectively multiplying the already immense data volume that needs to be managed.

To contend with these challenges, modern solutions combine hybrid cloud for effective high-volume data management with flexible cloud storage capabilities while having on-premises protection and control. To effectively manage these vast datasets of various types, automation has never been more important. Managed backups often function in a hybrid model that maximizes and simplifies the complexities of backup management while reducing the Total Cost of Ownership (TCO) along with ensuring that complete and accurate data is recovered quickly. Cost optimization approaches and tools that focus on eliminating duplicate copies are equally important when managing costs related to large datasets (Andrews, 2025).

The threat landscape has changed dramatically from cyber threats, and ransomware now ranks as one of the most prevalent and damaging threats to enterprise IT hardware systems. Cybercriminals have developed ever more sophisticated methods of encrypting or deleting an organization's data and then demanding a ransom for its return (Cloudian, 2025). A critical aspect of this evolution is ransomware's deliberate targeting and destruction of backup data, aiming to disable recovery options before the primary data encryption even begins (Connectwise, 2025). In this hostile environment, a viable option for data backup is necessary for businesses so that they may recover their data to a well and unaffected version while continuing their operation.

Immutable storage guarantees that the written data cannot be encrypted or deleted and is a strong defence against ransomware. As a result, organizations can restore their systems without paying ransoms. However, new resilience against data ransomware solutions is not limited to an immutable option, as we are now seeing a multi-tiered approach in protecting organizations against ransomware (Cloudian, 2025; Connectwise, 2025):

Offline/air-gapped Backups: this strategy involves physically or logically isolating data from the production environment and the internet, rendering it impenetrable to network-borne ransomware attacks; this serves as a critical "last line of defense".

Immutable storage (WORM): this technology prevents modification or deletion of data, even if administrative credentials are compromised.

Chain-free backup technology: unlike traditional backups that depend on a fragile chain of previous backups, chain-free backups ensure that each backup is a complete, independent, immutable snapshot. This means that if one backup is compromised, the others remain untouched and usable for restoration.

Endpoint protection on backup servers: deploying modern endpoint protection platforms on backup servers is crucial; these platforms can detect abnormal ransomware behavior as it begins to infect a system and can isolate infected systems.

Increased backup frequency: regularly increasing backup frequency minimizes the amount of data loss in the event of an attack, improving the RPO.

Regular testing in sandbox environments: ransomware recovery strategies must be regularly tested in controlled sandbox environments to ensure their effectiveness.

Encryption of backup data: comprehensive encryption of data both at rest and in transit is a fundamental security measure.

Multi-factor authentication: implementing MFA protects access to critical recovery systems.

Detailed incident response plans: a comprehensive, ransomware-specific incident response plan with clear protocols for communication, containment, eradication, and recovery is vital.

Real world examples provide clarity on these practices. Unitrends case studies provide countless examples of successful recoveries from ransomware, as well as many examples with organizations restoring encrypted files quickly and efficiently, often within minutes. Fundamentally, ransomware attacks have shifted backup from a data loss prevention component to a key segment of Cybersecurity defence, requiring a zero-trust relationship with the backup infrastructure. Ransomware resilience is a multifaceted, integrated solution that combines technical safeguards with protocols, and vigilant and engaged humans in the "fight", acknowledging that no one solution provides total protection (Connectwise, 2025).

A major impediment to enterprise data protection is the explosive phenomena of data sprawl. This goes beyond established concerns around enterprise capacity-storing data, affecting visibility of data as well as governance and extracting business value. Data is everywhere and anywhere, on-premises public and private clouds, at the core of the network, and increasingly at the edge. Securing data and searching for backups throughout that expanded landscape is a costly exercise, particularly when we are also trying to protect our responsibility of data governance and regulatory compliance.

A primary result of data sprawl is the inaccessibility of data stored across multiple, disparate media on-premises. This fragmentation makes it difficult to effectively analyse data, complicates migration, and makes it difficult to upgrade technologies, often resulting in significant downtime during recovery processes. Furthermore, the lack of scalability inherent in many traditional data storage solutions exacerbates the challenge of managing petabytes of data, especially when considering the need to create multiple backups for a comprehensive data protection strategy.

Modern organizations are leveraging hybrid cloud strategies to position their approach to higher volumes of data, therefore, dealing with data on sites cloud controlled stack. Cloud enables a more flexible scope of data volume appropriately within the world of data utility and chain of activities. Automation processes are still required to generate automated backup and recovery processes, as it is the streamlining of which data protection and recovery can be maximized across the diverse environments. Managed backup solutions play a pivotal role in simplifying backup management, reducing the TCO, and ensuring rapid data recovery by offloading these complex tasks from internal IT teams (Andrews, 2025).

4 Leveraging Advanced Technologies for Enhanced Resilience

Artificial intelligence (AI) and Machine learning (ML) are transforming data backup and recovery dramatically as these critical functions change from reactive processes to proactive, predictive, and self-optimizing processes. At a high level, ML is a subset of AI that allows systems to do data analysis without having to be programmed with specific steps to take. ML algorithms scour large volumes of historical data to find and learn patterns and relationships, and can predict new outcomes and trends, enabling proactive improvements to threat detection and response in data spaces.

These advances in AI and ML being applied to backup and recovery can manifest in a few different ways (Algomox, 2024): Predictive Analytics, Anomaly Detection, Intelligent Backup Schedules, Automated Data Recovery, Data Verification, Compliance Automation. Major cloud providers are increasingly integrating AI into backup services. For example, Google Cloud's Backup and DR Service uses Vertex AI to generate recommendations and specific solution paths (with step-by-step directions) and reference architectures (Google Cloud, 2024).

Overall, AI/ML moves data protection from a reactive, rule-based approach to a proactive, predictive, and self-optimizing system, forever changing the operational model of backup and recovery. Furthermore, it allows for more precise and smarter prioritization of data protection efforts, enabling mission critical assets to receive maximal resiliency and optimizing the allocation

of resources across heterogeneous data ecosystems. The advent of AI and ML in data backup and recovery has several transformative benefits, but it also has its own limitations and challenges that organizations should think through as outlined in Table 1. The transformative benefits of AI/ML in data protection depend on the ability to overcome some significant underlying challenges in data quality, model interpretability, and skilled expertise. Ethical and privacy-related issues arising from the usage of AI/ML in data protection, particularly with respect to sensitive data collection and the "right to erasure" introduces another dimension of compliance and trust responsibilities in terms of governance and "privacy by design."

Table 1: Benefits and limitations of ai/ml in data backup and recovery

Aspect	*Benefits*	*Limitations*
Cyber Resilience	proactive threat detection, real-time monitoring, automated responses, faster ransomware detection	inability to comprehend nuance, lack of relevant training data, overconfidence/bias
Operational Efficiency	automated tasks, reduced downtime, faster recovery, optimized storage, cost efficiency, continuous learning	high costs & complexity, shortage of skilled professionals, model operationalization/deployment challenges, accountability
Data Integrity & Compliance	data verification, compliance automation, continuous improvement	data quality issues, transparency paradox, privacy risks

Source: Tozzi, 2025; Algomox, 2024

Whereas immutable storage is an effective logical containment for data tampering, the evolution and sophistication of cyber threats, specifically ransomware targeting backup infrastructure, has necessitated developing more architectural protections in backup infrastructure: air-gap and chain-free backup architecture. That go beyond logical safeguards to physical or architectural isolation, producing layers of entrapment virtually impenetrable to network-based attacks.

An air-gapped backup is a method of data storage where critical data is copied and stored on media or machines that are "offline" and not practically accessible over the internet or the primary network. This defining isolation provides some significant advantages namely Network Isolation, Ransomware Protection, Data Loss Prevention, Enhanced Security Controls, Encryption and Hashing. Air-gapping methods today do not refer to simple tape formats either. Air-gapping using cloud technologies is on the rise where delayed access, MFA, honeypots, and/or separate credentials, creates a virtual barrier that simulates physical isolation within a cloud environment (Connectwise, 2025).

Many traditional backups follow a "chain" of backups such that each incremental or differential degree of backup is being referenced by specific memory that identifies the previous full backup degree. If the link is compromised or corrupt, all backups along that chain are corrupt, and the complete restore process can be compromised. Chain-free backup technology offers remedy to the weakness of the chain backup model, because each degree of backup is a full, independent, immutable data snapshot that is free from each incremental or differential backups relationships. Chain-free backups have three important key features: Independence, Resilience and Faster Recovery. When combined with immutable storage, air-gapped architecture and chain-free backups provide a "hardened, ransomware resistant data protection strategy", the multi-layered approach enables ransomware resiliency and deliver unrivalled peace of mind to the recovery points in the backups to enable quick restore of the business.

The air-gapped and chain-free back-up model development has emerged in response to significantly evolving cyber threats and the targeting of backup infrastructure with ransomware. This is an evolution that has pushed forth data protection beyond logical containment to understand and use some form of physical or architectural isolation (IBM, 2023b). The explorations, of

merging air-gapping and chain-free concepts, as well as utilizing cloud configuration, reinforce the point of how security-based concepts are being expanded and utilized as situational stimuli to support resiliency in hybrid cloud security postures, without decreasing scalability (Connectwise, 2025).

5 Regulatory Compliance and Industry Standards

In today's business environment, regulatory compliance is an essential consideration for the design and implementation of modern backup and recovery systems rather than an ancillary legal requirement. Failing to comply with international data protection and privacy regulation (e.g., GDPR, HIPAA, SOX, etc.) may result in financial penalty-related losses, legal liability, or reputational damage (IBM, 2023a). As a result, it is necessary to adopt a "security by design" and "privacy by design" approach to data protection (Acronis, 2022).

The GDPR is a broad privacy and data protection law created by the European Union to protect the personal information (PII) of EU citizens and requires businesses to be transparent about how they collect data and afford individuals substantial control over their personal data.

HIPAA is a United States federal law that outlines, among other things, how healthcare organizations and their business associates should protect the confidentiality, integrity and availability of Electronic Protected Health Information (ePHI).

The SOX Act was enacted as a response to corporate scandals that arose in the United States and is intended to hold corporations accountable and to enhance the transparency of corporations regarding financial reporting (IBM, 2023a). The SOX Act is primarily concerned with financial controls, but it has meaningful implications for the IT systems that support an organization's financial data.

Regulatory compliance has transitioned from an ancillary legal obligation to a key driver in the design and implementation of a modern enterprise backup and recovery system, necessitating the introduction of "security by design" and "privacy by design" concepts. The similarities in compliance demands associated with different regulations suggest they are trending towards a set of best practices with a singular liability tied to data protection. These regulations allow businesses to act on the operational security of a compliant backup modality (Table 2).

Cybersecurity frameworks address regulatory requirements and facilitate a structured, holistic, and comprehensive approach to protecting data and assisting organizations in building positive Information Security Management Systems. NIST and ISO 27001 are useful examples of frameworks that give organizations structure to support risk management and the continuous improvement of their tech backup as more than a stand-alone solution for an organizational IT strategy (Morrison, 2024; NIST, 2024).

NIST is an organization that provides guidance on risk management linked to cybersecurity risks. Specifically, it provides a taxonomy of high-level cybersecurity outcomes applicable to organizations. Although NIST conveys no prescriptive rules, it supports organization flexibility in their response to diverse organizational risks. The original cybersecurity framework (CSF) consists of five 'core' categories: Identify, Protect, Detect, Respond, and Recover (Morrison, 2024). The latest CSF (2.0) introduced a sixth 'core' category, "Govern," which is where organizations focus on strategizing, communicating, and monitoring the organization's cybersecurity risk management strategy (NIST, 2024).

Within the framework, the 'Protect' category includes many rudimentary elements of security, e.g., data encryption, and permission settings. The "Recover" function specifically covers all actions an organization takes to recover from a cybersecurity incident, including backup and recovery processes, post-incident reviews, and subsequent system improvements. NIST outlines the recommended actions for all backup and recovery processes, categorized within three pillars: planning, implementing, and testing. NIST specifies recommendations for implementations of specific technologies related to backup tasks, including recommended automation of backup

process for each of the different storage solutions, and participating in recommended data encryption technologies for data at-rest and/or data in-transit process (Morrison, 2024).

Table 2: Key regulatory compliance requirements for data backup and recovery

Regulation	Data Type Focus	Key Backup Requirements	Penalties for non-Compliance
GDPR	PII of EU citizens	encryption, access controls, audit trails, data retention, quick data recovery, right to erasure/access/portability, privacy by design, 72-hour breach notification	fines up to 4% of annual global turnover or €20m, legal action, reputational damage
HIPAA	ePHI	data availability & integrity, business continuity protocols, regular testing and revision, business associate agreements (baas), detailed documentation, audit trails, RBAC, automated backup verification, redundant storage, encryption	significant fines (up to $1.5m per violation category per year), criminal charges, reputational damage
SOX	Financial Records	data backup & recovery plans, financial records retention, tamper-proof storage, detailed audit trails, data accessibility, encrypted backups, RBAC, secure data deletion, regular testing	fines, imprisonment, legal action, reputational damage

Source: Acronis, 2022; Morrison, 2024; IBM, 2023a.

ISO 27001 is a global standard for security, and offers a complete and all-encompassing framework for planning, establishing, implementing, maintaining, continuously improving, and effectively using an Information Security Management System (ISMS) that permits the protection of sensitive information. Regarding data backup and recovery, ISO 27001 provides robust suggestions for sensitive information protection within a systematic backup process.

ISO 27001 routinely stipulates that acceptable requirements for backups of information, system images and relevant software data are required, all in accordance with an existing backup policy The ISO 27001 suggests backups should be arranged into a comprehensive framework, specifies responsibilities regarding backup verification, scheduling, and protections once the backup processes are complete. ISO 27001 risk assessment methodology assist an organization in evaluating and identifying risks associated with the backup context (Morrison, 2025).

Cybersecurity frameworks such as NIST and ISO 27001 can assist organizations in developing systematic, holistic methods of protecting data, supporting the transition from stand-alone reactive responses to backup and recovery systems, and developing integrated risk management and continuous improvement of those systems. The emphasis on "testing" and "documentation" within these frameworks highlights that the theoretical existence of backups is insufficient; their verifiable functionality and auditable processes are paramount for true resilience and compliance (Morrison, 2024; NIST, 2024).

Maintaining data integrity and availability in today's enterprise IT landscape is a complex process that necessitates a fully integrated multi-layered defence-in-depth strategy. The implementation of best practices across various security, compliance, and operational efficiency contexts because one single practice will not suffice in most situations. Key best practices include (Abnormal.ai, 2024; Connectwise, 2025; Zgureanu, 2021):

3-2-1 backup rule: this foundational principle advocates for maintaining at least three copies of data, stored on two different types of media, with one copy kept offsite .

Regular testing and validation: it is imperative to schedule routine restoration tests to verify backup integrity and ensure that data can be restored successfully when needed.

Automated backup processes: leveraging automated tools for backup processes reduces the risk of human error and ensures consistency.

Strong encryption: data must be encrypted both at rest and in transit to prevent unauthorized access.

Access controls: implementing strict authentication and authorization protocols, such as Role-Based Access Control (RBAC) and Multi-Factor Authentication, is essential to limit data exposure to only authorized personnel.

Data segregation and isolation: backups should be isolated from production environments to prevent cross-contamination: air-gapping provides a critical layer of isolation.

Clear retention policies: establishing clear policies that define how long backups are kept and when they should be deleted or archived is crucial for balancing storage space efficiency with compliance requirements.

Versioning and incremental backups: maintaining multiple versions of files and utilizing incremental backups optimizes storage usage and speeds up recovery processes.

Incident response plan: a well-defined data breach response plan is vital, outlining steps for communication, containment, eradication, and recovery.

Continuous monitoring and auditing: deploying advanced monitoring solutions to detect anomalies or unauthorized access attempts, conducting regular security and compliance audits, and reviewing access logs are essential for ongoing oversight.

Employee training: regular training of employees on data security protocols, current threats, and best practices for secure data handling is a critical human component of data protection.

The implementation of best practices across security, compliance and operational efficiency suggests that data integrity and availability is achieved through a holistic multi-layered defence-in-depth strategy and not use of singular action. The emphasis on "testing" and "monitoring" highlights a critical shift from merely assuming data recoverability to continuously verifying it, underscoring the dynamic nature of threats and the imperative for adaptive resilience.

6 Future Outlook and Market Trends

The outlook for today's backup and recovery options in enterprise information technology systems is one of continuous innovation, primarily driven by the ubiquitous introduction of AI and ML and the ongoing evolution of IT infrastructure to the edge. These technologies and trends are fundamentally changing how organizations think about data protection and resilience, including (Datto, 2025; Andrews, 2025):

AI-driven backup solutions. AI and ML are increasingly becoming part of backup solutions to predict failures, manage backup schedules, and improve data protection overall. AI/ML will continue to revolutionize cloud backup optimization through automation of repetitive tasks, guidance around decision making, and dynamic scenarios for backup settings using real-time data. Predictive failure, automated data classification, intelligent backup schedules, and stronger threat detection and response capabilities are all examples of AI and ML in backup solutions.

Edge computing. With data generation occurring more at the edge of the enterprise (IoT devices, remote offices, etc.), edge computing is increasingly critical for backup. It enables organizations to reduce latency and bandwidth costs by performing compute operations closer to where data is generated. This gives organizations increased speed and efficiency in backing up all levels of data. This decentralization of data processing and protection is a direct response to the challenges of data sprawl.

Advancements in cloud infrastructure. Continuous maturation of cloud is providing improved performance and reliability for backups. Improved speed of storage, security features, and cloud-native services are just a few examples of how the advancement of cloud infrastructure is enabling backup and recovery architectures that are scalable, flexible, and resilient.

Incremental forever backup. This method will continue to grow in popularity since it focuses on only backing up what has changed since the last backup while keeping a link back to that backup

version. There is a dramatically lower amount of redundant data archived while not sacrificing the veracity of any data restoration, resulting in a steady decrease of storage costs over time.

Hybrid backup solutions. Hybrid architectures will continue to be focused on, especially with their ability to simplify the work by allowing resources to be managed in one place, thus allowing legacy installations to be simplified. They will provide a layer of redundancy for Disaster Recovery and allow organizations to expedite recovery times for restores due to the faster recovery time of local versus cloud backups.

Ransomware-resistant strategies. With ransomware still being a threat, resistant strategies will continue to be a focus. This would include continued offerings and growth of immutable backups, air-gaps, encryption, and an incident response plan.

Unified backup trends. The insights provided by reports, such as "Unified Backup Trends 2025 Report", demonstrate that cloud adoption, data protection, and cybersecurity are converging and will be the key indicators moving forward in Business Continuity and Disaster Recovery (BCDR), indicating we are moving toward platforms that consolidate disparate systems to create data resilience. Leading vendors like Cohesity are recognized for their AI-powered data security and cyber resilience solutions, while Veeam is evolving its capabilities with technologies like GenAI and Microsoft Entra ID backup, emphasizing unified data resilience for diverse workloads.

The future of enterprise backup and recovery is expanding intelligence and decentralization due to the omnipresence of AI/ML and extending IT infrastructure to the edge. The convergence of data protection, cybersecurity, and business continuity into unified platforms is a dominant trend, reflecting a holistic approach to enterprise resilience in the face of increasingly sophisticated and integrated threats.

IBM Storage solutions showcase an eloquent example of real-world impact. Micro Strategies for example, used the IBM Storage portfolio to create "DataVault", a managed security services provider solution, which provides robust ransomware protection and safeguards critical client data against various data loss threats, enabling effective recovery from cyberattacks. There is also a case study that illustrated how IBM Solutions helped Data Action reduce its response time, which allowed their Security Operations Center to assess cybersecurity exposure and protect critical data and improving data resiliency (IBM, 2025).

This and other real-world implementations reinforce that modern-day backup and recovery strategies are not only conceptual, but real, concrete, and reliable solutions to business continuity, regulatory compliance, and cyber resiliency. They validate the effectiveness of advanced technologies and integrated approaches in safeguarding enterprise data in today's dynamic threat landscape.

Conclusion

Enterprise IT systems are constantly changing, with the driving factors being the significant increases in data volumes, a growing variety of data types across disjointed environments, and increasingly sophisticated cyber threats. Consequently, modern backup and recovery platforms have evolved from recreating data to providing businesses with digital insurance that is essential for operational resiliency and business continuity.

On-premises solutions provide the most direct control over the IT environment; however, they lack inherent disaster resiliency and extensive scalability. Cloud solutions allow the greatest granularity of scalability, accessibility, and offsite-protection, but at a price - dependencies and potentially unforeseen costs. With this trend towards hybrid architectures, often guided by the 3-2-1 backup rule, we have a path that combines the best of the ability to use intelligence in data tiering and automate management while optimizing cost, performance and redundancies.

Advanced strategies such as DRaaS and CDP are lowering the barrier to enterprise-grade resiliency. DRaaS turns disaster recovery from a capital intensive, in-house process into an agile, outsourced process with rapid RTO and RPO capabilities without the unnecessary upfront costs.

The distinction between DRaaS and BaaS is critical - true business continuity requires to be able to restore an entire operational IT environment quickly, not just a copy of some or all of the data. CDP captures data in real time, and provides near-zero RPO, which is a complete shift to continual data integrity. But using CDP comes with big infrastructure requirements and demanding operational management to limit single points of failure.

Immutable storage is a necessary key feature for modern data protection as ransomware threats and regulatory requirements rapidly emerge. Immutability ensures data cannot be altered, which effectively safeguards against ransomware and stays with regulatory compliance requirements. However, the cost and operational management are major factors for organizations to consider, they must have an awareness of data classification and retention. There is also physical or architectural separation, such as in air-gapped backup or chain-free backup architecture, that provide extreme resilience because they go beyond immutability and provide some kind of separation and isolation.

Regulatory compliance has changed from secondary consideration or value-adding, to primary consideration, alongside the regulatory requirements overall, regarding data protection design. There are common threads in these different regulatory requirements, which leads to general best practices for data integrity and availability, and highlights the need for organizations to adopt security by design and privacy by design principles. Risk management should also be seen through a larger lens, rather than ad hoc approaches, and cybersecurity frameworks like NIST and ISO 27001 provide structured and consistent ways to manage and achieve performance levels with the commitment to continuous improvement.

Intelligence and decentralization of primary data and system awareness will dominate the recovery and restore feature space for enterprises. AI/ML will continue to change the data protection landscape through predictive analytics, anomaly detection, and automated recovery processes, but legacy technology cloud-based applications or solution, still continue to evolve with a placeholder and human review/monitor.

Modern enterprise backup and recovery is a complex, multi-faceted discipline that demands a strategic, integrated, and continuously adaptive approach. Organizations must invest in a combination of foundational strategies, advanced technologies, and robust governance frameworks to build truly resilient IT systems capable of withstanding the challenges of the contemporary digital landscape.

References:

1. Abnormal AI., 2024. *Top ways AI enhances data backup security and recovery*, [online] Available at: <https://abnormal.ai/blog/data-backup> [Accessed 7 Aug. 2025].
2. Acronis, 2022. *GDPR compliance considerations for backup and storage infrastructure*, [online] Available at: <https://www.acronis.com/en-sg/blog/posts/gdpr/> [Accessed 4 Jul. 2025].
3. Algomox, 2024. *AI Automating Backup & Disaster Recovery in the Cloud*, [online] Available at: <https://www.algomox.com/resources/blog/ai_automating_backup_disaster_recovery_cloud.html> [Accessed 12 Jul. 2025].
4. Andrews, M., 2025. *Data protection trends in 2025 for MSPs and SMBs*, [online] Available at: <https://www.novabackup.com/blog/data-protection-trends-in-2025> [Accessed 22 Aug. 2025].
5. Arcserve, 2025. *Key components and best practices for an immutable backup framework*, [online] Available at: <https://www.arcserve.com/blog/key-components-and-best-practices-immutable-backup-framework> [Accessed 14 Jul. 2025].
6. Cloudian, 2025. *Ransomware backup*, [online] Available at: <https://cloudian.com/guides/ransomware-backup/ransomware-backup/> [Accessed 22 May 2021].
7. ConnectWise, 2025. *Immutable backup. The guide to ransomware-proof data protection in 2025*, [online] Available at: <https://www.connectwise.com/blog/what-is-immutable-backup> [Accessed 4 May 2025].
8. Datto, 2025. *Key takeaways from the unified backup trends 2025 report*, [online] Available at: <https://www.datto.com/resources/unified-backup-trends-2025-must-know-insights/> [Accessed 14 Aug. 2025].

9. Dropbox.com, 2025. *The advantages of using cloud backup*, [online] Available at: <https://www.dropbox.com/resources/cloud-backup-advantages> [Accessed 16 May 2021].
10. Google Cloud, 2024. *Backup and DR Service*, [online] Available at: <https://cloud.google.com/backup-disaster-recovery> [Accessed 15 Mat 2021].
11. IBM, 2023a. *Data Compliance*, [online] Available at: <https://www.ibm.com/think/topics/data-compliance> [Accessed 22 June 2025].
12. IBM, 2023b. *Disaster recovery*, [online] Available at: <https://www.ibm.com/think/topics/disaster-recovery> [Accessed 22 June 2025].
13. IBM, 2025. *Storage data backup and recovery solutions*, [online] Available at: <https://www.ibm.com/solutions/backup-recovery> [Accessed 1 Aug. 2025].
14. Morrison, R. (2024). *NIST Requirements for Backup and Recovery*, [online] Available at: <https://www.baculasystems.com/blog/nist-requirements-backup-recovery/> [Accessed 30 June 2025].
15. Morrison, R. (2025). *Implementing ISO 27001 Data Backup and Recovery Requirements*. [online] Available at: <https://www.baculasystems.com/blog/iso-27001-backup-recovery/> [Accessed 30 June 2025].
16. NIST, 2024. *The NIST cybersecurity framework 2.0*, [online] Available at: <https://csrc.nist.gov/news/2024/the-nist-csf-20-is-here> [Accessed 22 June 2025].
17. Zgureanu, A., 2021. *Backup and recovery strategies and their role in business continuity*, [online] Available at: <https://ibn.idsi.md/ro/vizualizare_articol/145534> [Accessed 30 Jun. 2025].
18. Zgureanu, A., 2022. *Rolul RTO și RPO în planificarea recuperării în caz de dezastru*, [online] Available at: <https://ibn.idsi.md/ro/vizualizare_articol/156521> [Accessed 29 June 2025].