White Paper

Advancing Data Protection Maturity: Considerations for 2023 and Beyond

Sponsored by: Veeam

Phil Goodwin
March 2023

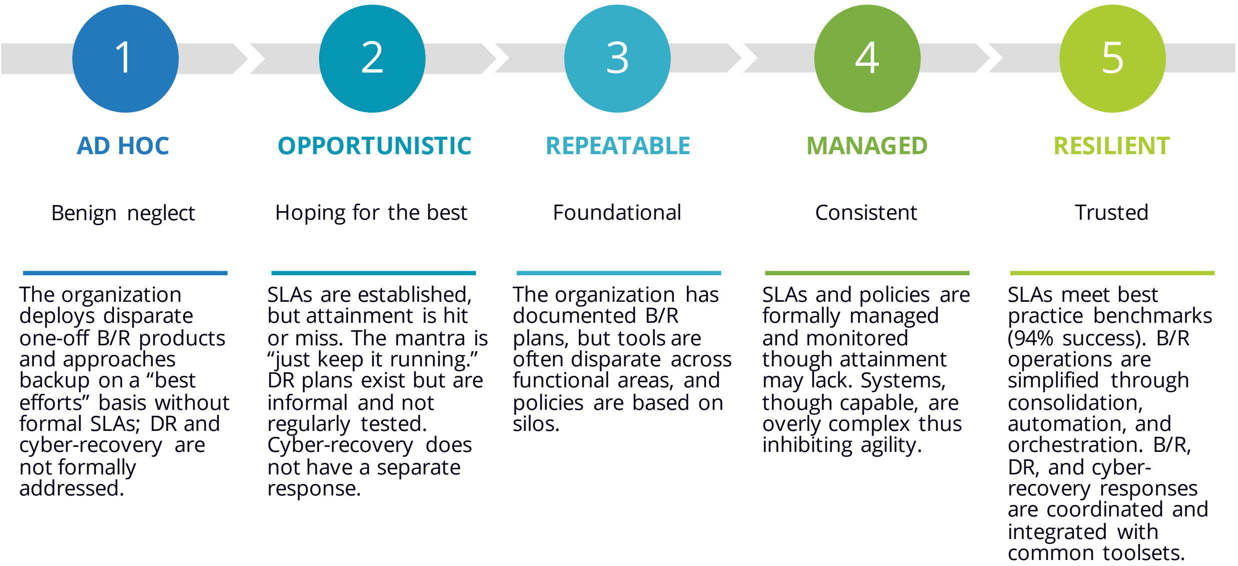
IDC OPINION

Backup and recovery (B/R) has been a core IT responsibility since the dawn of computing. In the earliest days, it was a simple dump from disk to tape with response times measured in days. B/R has evolved to address the needs of client/server architectures, then virtual infrastructure and now cloud and container infrastructure with ever greater sophistication and more stringent SLA expectations.

Unfortunately, B/R does not get the attention needed to transform it from being regarded as a necessary evil into a corporate strength. Indeed, those organizations that achieve excellence in B/R give their organizations a competitive advantage through better data availability and accuracy. There is a big difference between organizations that seek to keep B/R from being a liability (i.e., make it "good enough") versus those that seek to make it a strategic, competitive advantage. Our research shows that the continuum fits the common distribution curve with the majority being somewhere in the middle of the pack, whereby operations are formalized based on established processes but not to the extent of being optimized and regarded as trusted (see Figure 1).

FIGURE 1

Data Resilience Maturity Model



AD HOC	OPPORTUNISTIC	REPEATABLE	MANAGED	RESILIENT
Benign neglect	Hoping for the best	Foundational	Consistent	Trusted
The organization deploys disparate one-off B/R products and approaches backup on a "best efforts" basis without formal SLAs; DR and cyber-recovery are not formally addressed.	SLAs are established, but attainment is hit or miss. The mantra is "just keep it running." DR plans exist but are informal and not regularly tested. Cyber-recovery does not have a separate response.	The organization has documented B/R plans, but tools are often disparate across functional areas, and policies are based on silos.	SLAs and policies are formally managed and monitored though attainment may lack. Systems, though capable, are overly complex thus inhibiting agility.	SLAs meet best practice benchmarks (94% success). B/R operations are simplified through consolidation, automation, and orchestration. B/R, DR, and cyber-recovery responses are coordinated and integrated with common toolsets.

Source: IDC, 2023

The need for excellence in backup/recovery cannot be overstated. It is foundational to nearly every data-related initiative that organizations undertake, including digital transformation (DX), data availability, and digital acceleration. Competitive businesses rely on timely, accurate, and available information that cannot be achieved if B/R systems result in unrecoverable data and missed SLAs. To underscore this point, our research shows that nearly 50% of DX projects include data protection improvement initiatives, certainly addressing the need to keep B/R in sync with primary systems. One could also argue that until foundational IT services (like B/R) meet expectations, aspirational initiatives like digital transformation may remain out of reach.

Modern backup requirements have become increasingly complex. Organizations commonly have data located in private cloud, hybrid cloud, and multicloud (public) configurations. Many IT organizations must support applications in legacy systems (i.e., Unix and NAS), physical Microsoft Windows, virtual infrastructure, and Linux (both paid and unpaid). Further complexity is added by different data types, including structured databases, myriad unstructured file systems, email/collaboration platforms, and containerized data.

For organizations to realize their goals of data availability and business resilience, consistency of backup and recovery systems and operations is key. This includes consistent data protection capabilities and policies across applications and platforms, as well as reliable SLA delivery and consistent operational practices across the enterprise to reduce the opportunity for human error.

Operational consistency is a key part of data trust and requires organizations to pay attention to details. This consistency begins with a consolidated data protection toolset and policy engines that reduce silos and simplify operations. Mature organizations address B/R, disaster recovery (DR), and cyber-recovery holistically with common tools and operations. Whenever possible, having consolidated backup operations across platforms, and across on-premises, cloud, and data environments, pays dividends in reducing complexity and human error and improving quality of operations. Consistency results in measurable business outcomes, such as best practice SLA attainment of 94% or greater, reduced downtime as measured year over year, and minimized data loss.

SITUATION OVERVIEW

IT teams face significant challenges in their efforts to ensure trusted data resilience. Our research has found that organizations have an average of three backup tools, with some having as many as seven, often from multiple vendors. The impetus for these tool selections is often siloed data with separate administration and management policies that further complicate proper data governance efforts. Redundant backup tools also lead to inconsistent management policies, excessive maintenance costs, added training requirements, and complex operations.

Although a great deal of industry attention is being paid to ransomware — for very good reasons — the reality is that ITOps teams must deal with a wide range of data protection scenarios. These range from simple user error to hardware failure, software errors, and datacenter disruptions such as fires and burst pipes, all the way up to natural disasters. Malicious acts have become a major threat to data integrity and availability. These threats can be from external bad actors and their malware, but IT leaders should not ignore internal threats and should be prepared to defend against them. In addition, accidental user error has plagued IT since the beginning of computing.

Addressing the range of threats requires that organizations deploy layers of data protection technologies. Backup is the foundational component, but organizations also supplement backups with snapshots, replication/clones, cloud tiering, and other data copy methodologies to ensure data survival against the myriad threats. Policies affecting different data types can also require such actions as encryption, immutability, and air-gapped copies. As a cautionary note, however, these technologies are often vendor or system specific, meaning they are managed individually, which can lead to inconsistent implementation and increases the chances for human error.

Data protection platforms have emerged to consolidate data protection efforts and reduce the challenges of system-by-system protection schemes. Many of these platforms include copy management as well as recovery orchestration tools that automate recovery and leverage the fastest possible recovery path.

Driving all of these factors are ever more stringent service-level requirements and the need to both reduce downtime and minimize data loss. Although zero-RPO and zero-RTO are unrealistic today, organizations are getting closer and closer to this ideal state. Currently, the best practice RPO is 15 minutes with a 1-hour RTO, although this may vary depending on the application, data volume, and so on. Life-and-death systems may require far more stringent SLAs, but they are the exception.

The combination of hybrid cloud, multicloud, and SaaS application deployments — a scenario faced by more than 90% of organizations — introduces additional complications to effective data availability and backup. This is especially true for SaaS applications where the common "shared responsibility" model makes the customer responsible for the protection of their data even though the system is managed by the SaaS vendor. Too often, IT administrators and executives may erroneously assume that data in the cloud is automatically backed up and properly managed. Moreover, business users, who often are the subscribers to SaaS apps, generally are not savvy to data protection or governance requirements, and thus the SaaS apps and organizational data may go unprotected. When SaaS data is backed up by the vendor, it is usually for the vendor's purposes to rebuild its environment in case of a catastrophic event within its service; those backup's governance policies and SLAs rarely meet corporate-world standards. Unless data protection is explicitly provided, users should assume SaaS and cloud implementations only include the most basic backup provided by the cloud provider and anything additional (i.e., multiple data versions or medium-/long-term retention) is entirely the subscriber's responsibility. IT managers should also be aware that cloud implementations almost never have built-in DR or cyber-recovery contingencies, so it is fully the responsibility of the IT organization to implement them as needed.

Because of the changing nature of application deployments and the evolutionary changes that open vulnerabilities, IDC recommends organizations undertake the following initiatives:

1. Bottom-up analysis data protection activities beginning with threat analysis and matching the threats to backup and recovery schemes along with service-level requirements, jointly conducted between IT and business stakeholders
2. Gap analysis on areas of vulnerability, with special examination of hybrid cloud, multicloud, and SaaS
3. Global policy review regarding data protection and governance requirements
4. Disaster recovery and cyber-resiliency capabilities layered on top of a foundation of backup and recovery

FUTURE OUTLOOK

When seeking to enhance an organization's backup maturity, IT leaders can utilize the IDC Data Protection Maturity Model to describe the processes and outcomes. Given the diverse IT and business landscapes that organizations must navigate along with threats that must be protected against, IT leaders should be planning to address three key areas in 2023 and beyond:

- **Cyber-resiliency.** With cyberattacks so pervasive, common, and destructive, it is recommended that data protection toolsets integrate with cyberdetection mechanisms during backups and restores. Backup systems are reactive in nature, but organizations need a more proactive posture. Thus it is critical that cybersecurity teams (SecOps), backup teams (ITOps), and overall IT leadership are aligned on prevention policies, preparation methods (i.e., testing backups for whole-scale restorations), and the roles and procedures that the respective teams will take when a cyberattack occurs.
- **Hybrid/multicloud.** As workloads move from the datacenter to a cloud, or back on prem, or from one cloud to another, data protection toolsets and strategies need to ensure the data remains protected. Ideally, the same vendor or technology base that protects the datacenter workloads would also protect the cloud workloads (or vice versa) so that skill sets are retained and data is neither overprotected (two teams doing it) or underprotected (both teams assuming the other is).
- **Backup maturity mentality.** Immature organizations focus on backup, but more mature teams design for restore, not just backup with a focus on SLA delivery. In addition, per the maturity model, orchestration of recovery tasks, automated testing/validation of backups, improved documentation for operational and regulatory adherence, and so forth should not be considered "optional" enhancements.

CONSIDERING VEEAM

The Veeam Data Platform is designed to provide enterprises with a breadth of support for today's diverse workloads. Additional products further extend this platform to protect SaaS solutions as well as Kubernetes environments.

Key products in Veeam Platform include:

- Backup and recovery that helps IT teams own, control, backup, and recover all corporate data, anywhere in the hybrid cloud or multicloud
- Monitoring and analytics that enables real-time visibility, improving recovery success with proactive management
- Recovery orchestration that provides application, server, and even full-environment disaster recovery with up-to-the-minute RTO, RPO, and SLA monitoring

CHALLENGES/OPPORTUNITIES

Modern IT environments are so diverse that addressing every scenario is nearly impossible for any data protection product. To meet these diverse needs, the data replication and protection market remains dynamic and robust. IDC identifies more than 40 vendors in the data replication and protection software market, many of which are boutique companies specializing in very specific areas with a focus on "best of breed" for their niche. As part of its research, IDC has identified Veeam as a leader in this critical market segment. Thus Veeam finds itself competing in a very crowded market against both much larger companies and highly focused smaller companies. To continue to be successful, Veeam must battle on both fronts by providing both broad platform support and focused product capabilities.

The nature of data protection is also constantly evolving. New threats emerge, new platforms are deployed with new technologies, and new applications are constantly emerging. Veeam must address these emerging requirements on a timely basis to avoid customers with unsatisfied needs, or worse, open vulnerabilities.

Because no company can "do it all," building partnerships and developing a complementary ecosystem is crucial to ongoing success. Much of Veeam's success to date has been the result of a vibrant ecosystem of complementary service providers and partners. Maintaining this ecosystem will continue to be a critical success factor for the company.

CONCLUSION

Few organizations consider themselves to have truly "trusted" data protection systems. Rather, most fall somewhere earlier on the data protection maturity spectrum. However, those organizations with superior data protection strategies are able to deliver better data availability and accuracy, which will yield marketplace advantages.

Much current market attention and hype is being given to ransomware, and indeed, ransomware is a serious issue that IT organizations must address. Nevertheless, IT teams must not divert their attention from the day-to-day backup and recovery demands. Although ransomware is a constant threat, it is still far less frequent than more common data loss events such as hardware error, software failure, and simple user error.

Backup and recovery remains the foundation for data availability and protection. Without solid and reliable backup systems and operations, other efforts will be ineffective. And, while cloud has been a game changer for data protection in many ways, it is no panacea or magic bullet for ensuring data survival; organizations still need enterprisewide data protection solutions, solid processes, and comprehensive contingencies. By frankly assessing where an organization sits regarding data protection maturity, leaders can then lay out a path of improvement regarding strategy, tool selection, and vendor alignment.

MESSAGE FROM THE SPONSOR

Watch a demo of all the Veeam Data Platform capabilities here.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com