The 8 Keys to Database Protection for SQL Server DBAs

By **Joseph McKendrick, Lead Analyst**
Produced by **Unisphere Research**,
a Division of **Information Today, Inc.**

Sponsored by

Produced by

Table of **Contents**

Today's organizations rely on their data for everything from fundamental administrative processes to developing new strategies and innovations. As one of the key stewards of its data, organizations depend on SQL Server DBAs to ensure data is available, accessible to those who need it, and protected from threats. This report defines the challenges that SQL Server DBAs face in supporting that objective and offers solutions on how organizations can help them.

Digital Transformation Requires Cyber Resiliency for SQL Server Databases

Imagine running a high-volume digital business, performing thousands of transactions an hour with customers all over the world, and having your data center—or even cloud provider—suddenly go dark. Maybe your enterprise was suddenly hit by a ransomware attack, locking away the key data assets that support critical business processes. Or maybe a system error left thousands of your customer transactions in limbo.

Organizations of all kinds, from retailers to healthcare providers, have digitized their operations, services, and even products to become faster and more efficient. As a result, they now need data to accomplish even basic operations, such as accounting for inventory or managing payroll. If data is inaccessible, business stops. So, organizations need to protect their data not only to compete in the digital economy, but also to simply function.

Digitizing work, or moving physical products and manual operations to online environments, has led organizations to become highly distributed. Employees no longer need to work at single, on-site locations. They increasingly rely on multiple systems across interconnected business units for the transfer of essential information. So, enterprises need to manage and retain significant amounts of data across many systems and locations.

To ensure that they can maintain 24x7x365 availability despite technical incidents and cyberattacks, enterprises need to be able to address issues with minimal disruption. By making its data resilient, an organization can keep data available and accessible at all times, even during an unexpected event like an outage or a cyberattack.

Not only does proactive data resiliency play a vital role in keeping a business running, but it's also foundational for meeting compliance requirements, particularly in light of new data privacy mandates, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Regulations such as these require that sensitive data be physically maintained within national borders, as required by GDPR, as well as auditable and closely monitored for security breaches, as with CCPA. Lawsuits can also trigger information discovery for which organizations must have pertinent data on hand when needed.

Data resiliency is crucial for maintaining business continuity and compliance, but it isn't easy. For example, a DBA may understand the location and domain of data within their

enterprise, but to achieve resiliency in a cost-effective, expedient way, they need to also understand the information's importance and context. Is it sensitive data? Is it of material importance to the business? Is it data that needs to be available within sub-seconds to end users or applications, or is there room for latency?

The repercussions for not meeting these business and compliance requirements can be felt across an organization, including the boardroom. Even less severe GDPR infringements can result in a fine of up to €10 million, and the impact of a ransomware attack can extend well beyond the actual ransom cost—and any fines—when downtime, remediation, and loss of consumer trust are tallied. Moreover, the cost of outages as a whole is climbing. A quarter of respondents to the 2022 Uptime Institute Global Data Center Survey, said their most recent outage cost more than $1 million in both direct and indirect costs, a significant increase from 2021.[1]

As guardians of their organizations' most valuable data, the responsibility for fulfilling the goals of data resiliency is increasingly falling on the shoulders of DBAs. At the same time, many database teams are already stretched thin with an ever-expanding list of duties around managing data environments that continue to grow in size and complexity across on-premises and cloud sites. Nearly three-quarters of DBAs surveyed recently by DBTA reported that the number of databases they manage has increased, and 42% indicated that the expansion of their duties has been significant. Moreover, 51% of respondents said that turnover has been "above average" in the past year.[2]

In an era of ever-rising cybersecurity threats and business demands, it is increasingly clear that DBAs need a better way to ensure data resiliency while managing their many other responsibilities. In this report, we'll discuss how DBAs can streamline their work and make their data resilient with modern backup and recovery solutions.

Data Security Is Now Everyone's Job, and DBAs Must Take Charge

In the past, data security was not a major part of the average DBA's job. While controlling user access has always been important, security at large was viewed as the domain of specialists. When compared to traditional DBA responsibilities, such as database maintenance and performance monitoring, security was lower on the priority list and comprised a fairly limited area of activity. Today, DBAs are spending more time on security than anywhere else.[2]

This shift is the result of a variety of trends converging to reshape the role of the DBA. Over the past decade, the volume of data, the number of sources that produce data, and endpoints on which data is stored have all grown significantly. To maximize the value of their data, organizations have invested heavily in technologies to capture and store data and deliver quick and easy access to data among employees, partners, and customers. This ease of access also comes with a responsibility to keep data secure, which means that security is no longer the purview of one team, but many teams across an organization, including DBAs.

Since DBAs are charged with assuring the quality, reliability, and availability of data, they are uniquely positioned to play a more expansive role in combating security risks and threats. From database hardening and encryption to patch and password management, DBAs have the expertise to optimize processes and practices to improve the protection of data. Moreover, without DBAs laying the necessary groundwork, the work of security teams will only go so far. That is why integrating security into applications and systems early in the design and implementation stages has become a best practice. This broadens the scope of security across many stakeholders within an organization to tackle it together proactively.

The increased focus on security among DBAs nowadays is also related to a larger movement taking place within organizations. The adoption of cloud platforms and services has opened the door to the automation of many routine data management tasks. When organizations move from an on-premises database to a cloud database, there are often significant changes to the DBA role. These changes can require new skills. However, they also present an opportunity for DBAs to move up the value chain by moving away from redundant work that takes up valuable time and toward activities that more directly support business goals.

Ultimately, today's digital businesses depend on the availability, integrity, and confidentiality of their data to make decisions, power their applications, and keep their operations running. Cyberattacks and outages are increasing in prevalence and cost—a looming threat that needs to be managed proactively and collaboratively. The DBA role is evolving as the result of both technology and business trends, and security has emerged as a key responsibility. As businesses rely more heavily on DBAs to deliver both a competitive edge and guard the data that will help ensure that edge, DBAs need to be empowered with solutions that enable them to work faster, smarter, and more flexibly to both manage and protect data.

Complexity Creates Cybersecurity Risk

SQL Server databases are complex and interface with many parts of the enterprise and well beyond. Today's SQL Server enterprises also have many endpoints and many users who may be fallible to often insidious social engineering tricks that can provide malicious parties access to their organizations' backend systems and information assets. These parties can then use this access to launch ransomware attacks that bring organizations to their knees by seizing and encrypting critical data.

These data breaches come at a huge price. The average cost of a data breach climbed almost 13 percent between 2020 and 2022—from $3.86 million to $4.35 million—according to a survey by Ponemon Institute. The survey also found that 83 percent of responding organizations had more than one data breach.[3]

But the costs of resolving a data security breach go well beyond simply patching up affected systems. There may be legal implications and compliance violations if the breach affects customer data. A breach may also negatively impact customer or market trust, which has long-term implications on revenue.

Backup and recovery practices have been around for decades, and there is no one-size-fits-all data protection strategy. Each organization must establish policies that identify what data and systems need to be protected; how often and when backups should occur; how and where backups should be stored; how long backups should be retained; restore procedures; testing and monitoring procedures to ensure compliance with SLAs; and key roles and responsibilities.

Backup and recovery success is measured in two ways: recovery time objective (RTO), or the maximum amount of time it takes to restore operations after an attack or failure, and recovery point objective (RPO), or the amount of data an organization can tolerate losing in such a situation.

The traditional method of backing up data at an organization's primary site to disk storage is still widely used today. In many cases, tapes are also employed for archiving or disaster recovery. It's also quite popular for SQL Server database customers to replicate data to secondary sites for business continuity. However, this traditional approach also involves numerous components—both software and hardware—which create more complexity and a higher risk that human error or the failure of one dependency will disrupt the entire operation.

At some organizations, DBAs maintain complete control over backups. But managing backups can eat up a considerable amount of their time. At other organizations, this responsibility is delegated to backup administrators. But this division of labor presents its own challenges.

Databases often hold information that supports critical business functions. So, DBAs are wary of any process that has the potential to degrade the performance of their databases.

On top of that, because they often don't have access to the backup tool itself, they also want to ensure that their backup data is properly configured in case they have to use it for a recovery. As a result, DBAs commonly prefer to back up their own data and "dump" it somewhere for a backup administrator to "sweep" it into another location for retention, in an approach known as "dump and sweep."

Again, because their databases are so complex, and yet so critical to the organization, DBAs also want to manage any necessary recoveries. But because they don't have access to the backup tool, they're reliant on the backup admin to pull the data required for recovery.

This divide can create a number of issues, including: disjointed processes, increased storage costs, and lost productivity.

For many SQL Server DBAs, backups involve far too much manual scripting and job scheduling. Plus, the growth and sprawl of data has resulted in data assets extending well beyond the confines of SQL Server databases. This makes managing backup and recovery a far more complicated and time-consuming process.

As a result, traditional backup and recovery solutions are no longer adequate for addressing the data protection needs of today's organizations. The data environments for which they were originally designed have evolved beyond their core strengths—as have the responsibilities of DBAs for which these tools no longer sufficiently help manage and protect data from outages and ransomware. The ongoing need for manual processes makes these solutions slow and error prone. The high capital costs and lack of ransomware protection are also significant drawbacks in today's business environment.

An SQL Server DBA's Top Challenges

DBAs are pressed to keep their databases secure and available at all times. But they simply have too much on their plates to do this effectively with the traditional tools they currently have.

Here's a summary of the challenges that DBAs face:

- **DBAs are under more pressure to keep data available and secure.** Organizations need data to function. But security threats are pervasive today. And since digital enterprises have more data in more locations, the "attack surface" of enterprise systems has expanded dramatically. DBAs need to be able to assess ongoing risks faster and smarter and work with their businesses to put proper controls and solutions in place.

- **DBAs need to manage increasingly complex data environments.** SQL Server databases interface with many parts of the enterprise across on-premises, hybrid, and multi-cloud environments. Most SQL Server shops have a plethora of different types of databases and applications that are connected to each other. Cloud has also made data environments more diverse and interdependent.

- **DBA time is too valuable for routine, day-to-day tasks.** DBAs today are expected to do more with less as database sprawl and cloud adoption have upped the level of heterogeneity and complexity. Maintaining and managing backups across different databases and data types is difficult and time-consuming, especially with native tools that are only suited to specific database engines, like SQL Server's Volume Shadow Copy Service (VSS). This time commitment restricts the ability of DBAs to focus on more strategic initiatives. DBAs need a way to limit the amount of effort they put into managing backups while still being able to quickly recover their data as needed.

- **DBAs need to embrace automation, but still retain control over their data.** With legacy solutions, DBAs either spend too much time managing their own backups or need to rely on backup administrators to do it for them. In the latter scenario, DBAs may follow a dump-and-sweep approach, where backed-up data is "dumped" into available storage, then "swept" into more permanent storage. However, this can result in each team potentially following their own procedures, requiring their own storage, and leading to conflicts.

- **Data environments need to be responsive to the business.** It is important to service the data needs of secondary users—developers, auditors, business analysts—who frequently ask DBAs for access to data to help them meet their business objectives. DBAs need to be able to fulfill these requests quickly and efficiently. With traditional solutions, many DBAs spend time and energy working with backup administrators to find the proper backup, as well as negotiating with the storage team for the necessary capacity to recover.

How a Modern Backup and Recovery Solution Can Empower DBAs

Data protection that's built on modern data backup and cyber recovery technologies can help businesses keep data secure and support strategic initiatives. With these technologies, DBAs can get their time back while also ensuring rapid recovery. The following list contains recommendations on how organizations can help DBAs meet the needs of their fast-evolving environments:

1. **Provide DBAs with pain-free backup and recovery options.** DBAs need to ensure that they have a clean, up-to-date copy of their data available at all times in the event that they need to do a restore. But they also don't have time to manage complex backup processes. With the right tools in place, DBAs can get their time back, while also retaining confidence in their ability to restore data.

2. **Automate everything.** Many of the tasks associated with supporting complex enterprises are too overwhelming for the scripting approaches that many DBAs used in the past. Automation can bring these pieces together, especially from disparate database environments.

3. **Keep DBAs in the driver's seat with flexible recovery options.** Organizations often have multiple types of databases serving different functions—from centralized SQL Server environments to NoSQL and open-source databases. On top of the engine variety, not all databases are created equal in terms of importance. Modern backup and recovery solutions give DBAs the ability to tailor recoveries across their environments to meet the needs of their businesses.

4. **Make it easy to prove they can recover their data.** One of the challenges within today's enterprises is the need for 24x7 reliability. DBAs can ensure this reliability if they have the ability to easily oversee whether backups ran, check the latest recovery points, and validate backups to ensure that restores will actually work in the case of a catastrophic event.

5. **Standardize on a single platform.** Ideally, both DBAs and backup admins would use a single solution in order to simplify operations and overall compliance. If both teams can use the same platform, they can have better visibility over the entire environment and prevent duplicative processes. A single platform also makes it easier to manage SLAs through automation.

6. **Help them quickly fulfill secondary user requests.** While managing the performance and availability of business-critical applications and systems and navigating the changes and challenges of the evolving landscape of database management, DBAs are also expected to help fulfill an ongoing stream of requests from secondary users seeking copies of production data for a range of activities, such as testing and development, ETL, audits, and analytics. DBAs need solutions that help them maximize the value of

backup data with rapid access to that data and the flexibility to integrate it with existing processes and tools. These capabilities will increase DBA productivity towards enabling new projects and initiatives that add direct value to the business.

7. **Help them use the cloud safely and strategically.** To effectively manage and protect data today, DBAs need a single platform that can handle an organization's entire heterogeneous environment, including their cloud databases. DBAs can also use the cloud for long-term data retention, which provides rapid access to data without the latency issues formerly involved with tape-based archiving. Long-term data retention in the cloud helps organizations better manage storage and infrastructure costs as well.

8. **Look to APIs.** As organizations have invested heavily in digital transformation and the adoption of new cloud and web-based technologies, APIs have emerged as the building blocks and connective tissue of the digital world. From DevOps to data management, the introduction of APIs enables the automation of operations by offering access to predefined processes, which frees up time and resources. To ensure applications can easily interface with each other, API-first development models have become increasingly popular. Modern backup and recovery solutions built with an API-first architecture benefit DBAs by providing them the ability to not only easily integrate with popular tooling, but greater flexibility in enabling self-service automation.

How Rubrik Delivers a Modern Backup and Recovery Solution

Rubrik pioneered Zero Trust Data Security™ to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions.

Rubrik Security Cloud, a modern backup and recovery solution powered by machine learning, delivers data protection and cyber resilience in a single platform across enterprise, cloud, and SaaS applications. The platform automates policy management of data and enforcement of data security through the entire data lifecycle, so SQL Server DBAs can spend more of their time on high-value projects.

Rubrik Security Cloud can help DBAs and the organizations they support:

- Preserve data integrity and keep data readily accessible to withstand cyberattacks, malicious insiders, and operational disruptions.
- Surgically and rapidly restore impacted apps, files, or objects by containing threats and orchestrating recoveries while avoiding malware reinfection.

To find out how Rubrik can help you enhance data protection for your database environment and increase the productivity of your entire team, visit rubrik.com/databases.

[1] *Uptime Institute Global Data Center Survey, https://uptimeinstitute.com/resources/research-and-reports/uptime-institute-global-data-center-survey-results-2022*

[2] *Information Today, The State of the Data Environment and Job Roles, 2022, Joseph McKendrick, May 2022*

[3] *Cost of a Data Breach 2022: A Million-Dollar Race to Detect and Respond, Ponemon Institute and IBM. https://www.ibm.com/reports/data-breach*

About Rubrik

Rubrik is a cybersecurity company, and our mission is to secure the world's data. We pioneered Zero Trust Data Security™ to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, delivers data protection and cyber resilience in a single platform across enterprise, cloud, and SaaS applications. Our platform automates policy management of data and enforcement of data security through the entire data lifecycle. We help organizations uphold data integrity, deliver data availability, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

Visit rubrik.com/databases to learn more.