CENTER FOR DIGITAL GOVERNMENT

DESIGN, MANAGE & SECURE:

A Game Plan for Public Sector Data Management

VOLUME TWO: PUBLIC SECTOR DATA MANAGEMENT SERIES

Louisville, Ky., combines information collected from the city's traffic sensors with a data feed from the navigation app Waze to detect traffic problems and identify the impact of signal timing and lane changes on traffic flow.

INTRODUCTION

Data has become the lifeblood of government. Utah uses data to monitor unemployment insurance systems for fraudulent activity, while data helps Indiana identify potential savings in the state's Medicaid program. Louisville, Ky., combines information collected from the city's traffic sensors with a data feed from the navigation app Waze to detect traffic problems and identify the impact of signal timing and lane changes on traffic flow.[1] And Pittsburgh uses data to address a variety of community health problems and safety improvements.[2]

These operation and citizen service improvements will continue as governments deploy more smart devices as part of the Internet of Things (IoT) and leverage more data feeds, applications and analytics. At the same time, citizens, business owners and community organization leaders will have higher expectations for data transparency and accessibility.

This flood of data has moved governments quickly from gigabytes to terabytes and now petabytes, which exceeds many agencies' existing storage capacity. Several trends are contributing to this and impacting an agency's approach to data storage, management, and security practices and technologies.

DIVERSE DATA TYPES.

Unstructured data such as images, audio and video adds complexity to storage and management requirements, particularly due to large and variable file sizes.

HIGHER USER EXPECTATIONS.

Constituents expect easy, responsive online access to general agency data, especially in an open portal — yet only 21 percent of governments have a mandatory open data initiative in place.[3] Citizens and businesses also expect the ability to see and update their own information online, such as when making a payment, obtaining a license or accessing services.

MORE REGULATION.

State and local agencies have had to comply with federal privacy laws for some time. But now, more states are enacting their own privacy laws, as well as data management and retention mandates. Expanding regulatory requirements mean agencies need to ensure they can effectively sustain and prove compliance.

ONGOING SECURITY CONCERNS.

Government data stores continue to be an appealing target for information theft because they contain the valuable personal information of employees and citizens.

Agencies can keep pace with these ever-expanding data challenges by applying a three-phase strategy: design, manage and secure. During the first phase, agencies design on-premises and cloud resources to optimize data storage, access and recovery. In the second, they apply governance practices to improve data management and regulatory compliance. And in the third, agencies adopt a standards-based framework and storage technologies to build a strong foundation for data security.

"We believe governments that adopt these strategies faster can reduce the cost of operations and avoid the need to look for new revenues," says Doug Snyder, a distinguished engineer with Veritas.

This handbook will outline what agencies must do to design, manage and secure data, and the strategies, tools and approaches for doing so within the constraints of limited staffing levels and tight budgets.

Phase 1: DESIGN

The Hillsborough County Circuit Court in Florida maintains a backup system for its virtual machines, physical and SQL servers, and its Microsoft Exchange system.

Data storage can be complicated in public sector organizations. There is often no coherent, enterprise-level design, and an agency may have data storage scattered across numerous systems and applications, both on premises and in the cloud. As a result, data is harder to access, share and secure; harder to manage for compliance; and harder to restore after a disruption.

A comprehensive and proactive data storage design can address many of these challenges. It also helps agencies combat infrastructure sprawl, make a gradual and sensible migration from legacy systems, and be ready to both accommodate and take advantage of more digital information to come.

A data storage design also offers several benefits for IT, including:

- Full visibility into all data systems, whether on premises, in the cloud or in hybrid environments
- Assurance that the right applications, both internal and external, can access each data system easily and securely
- Identification of business continuity plans and solutions that will be effective regardless of where data resides
- Ability to properly and efficiently manage data for access and retention compliance, as well as public records requests
- Easier transition of appropriate data to the cloud and ability to scale storage systems to accommodate data growth

THE RIGHT DATA STORED IN THE RIGHT PLACE

Cloud-based data storage is a viable option for public sector organizations to consider, and many have already migrated some data to the cloud. However, a successful move requires a design that fully explores how to optimize data storage across in-house data systems, as well as private, public and hybrid clouds.

There are many benefits to using cloud storage, including flexibility, scalability and cost savings. However, there is also a trade off to consider — cloud can add complexity, especially when an agency uses multiple services from different vendors.

For example, cloud vendors typically define multiple storage types (and costs) based on the level of needed access. These levels make it important to consider how often the data is accessed and updated. The cloud may be best used for infrequently accessed archive data, while active data remains in house.

Interoperability among all storage types used by the agency will also be an important design factor. A well-considered storage design helps IT ensure data is stored in the right places with the right controls, and that it is platform and vendor neutral.

The Hillsborough County Circuit Court in Florida maintains on-premises storage systems but is exploring cloud options for data storage.

“We know we will eventually move some things to the cloud and our storage and backup architecture will allow us to do that easily,” says Scott Cutler, system software manager for the court.

Stakeholder education across the agency is an important part of cloud exploration.

“You need to develop an organization-wide understanding about how to best use the cloud for data storage,” says Jarrod Klimek, senior storage and VMware administrator for the court.

> **When we looked at how we could make our backup environment more efficient, we decided to consolidate on a single vendor's solution end-to-end. We gained a system that is very efficient, very fast to patch and upgrade, and easier to manage.**
>
> — Jarrod Klimek, Senior Storage and VMware Administrator, Hillsborough County Circuit Court, Fla.

A common misperception is that cloud storage is suitable for all data types and storage needs. But the complexity and compliance requirements that come with government work may mean that some data will need to be kept in on-premises systems. Defining an "exit strategy" before moving that data to the cloud can avoid headaches if data needs to be brought back to internal systems in the future.

OFTEN OVERLOOKED: STORAGE DESIGN FOR BUSINESS CONTINUITY

As more portals and commercial applications rely on access to government data, the performance of that data becomes critical. Reliable data access is also vital for internal applications, analytics and automated processes.

"If you're creating an expectation that certain data will always be available, what happens if it's not?" says Michael Sherwood, director of innovation and technology for the city of Las Vegas. "You need to be ready to handle data that is lost, inadvertently deleted or altered."

IT teams often have a data backup and disaster recovery strategy, but they don't always plan for the data access capabilities that enable business continuity. One reason: The cost of needed system and network resources for high-availability and failover operations. It's important to prioritize business areas and use automated functions wherever feasible to create a continuity plan and storage infrastructure that balances continuous data access with resource expense.

However, it's not just data feeds or traditional documents, databases and records that need to be protected by a backup and continuity design. The Hillsborough County Circuit Court also maintains a backup system for its virtual machines, physical and SQL servers, and its Microsoft Exchange system.

"When we looked at how we could make our backup environment more efficient, we decided to consolidate on a single vendor's solution end-to-end," says Klimek. "We gained a system that is very efficient, very fast to patch and upgrade, and easier to manage."

Regardless of where data resides, best practices for sustaining continuous access include:

- Planning for disruptions in all data storage resources, even virtualized and cloud
- Supporting remote data recovery through automated processes to avoid reliance on manual actions by on-site staff
- Prioritizing continuity needs and resources to make the best use of limited budgets
- Regularly testing continuity systems, services and processes

SOLUTIONS FOR BETTER DATA DESIGN

An effective data design depends on the ability to see and manage data across all agency systems. Veritas solutions provide global visibility, centralized management and mission-critical protection for data stored across diverse systems and environments.

☒ **NETBACKUP:** Reduces the complexity of enterprise data protection through a unified solution built on converged infrastructure; scales with relentless growth through best-in-class performance at petabyte-level capacity; and paves the way to IT-as-a-Service through convenient, self-service operation. It lays the foundation for universal data management, enabling rapid visualization of data and accelerating cloud adoption with minimal risk. This solution also integrates with Veritas Information Map or Data Insight for increased data visibility and with the Veritas Resiliency Platform for service continuity.

☒ **NETBACKUP STORAGE APPLIANCES:** Integrate simple and effective backup, storage and de-duplication functionality on the device. The appliances reduce costs by streamlining storage management, operation and support and address changing requirements with easily scaled capacity and performance as well as the ability to quickly deploy new data protection capabilities.

☒ **INTEGRATED CLASSIFICATION ENGINE:** Provides the ability to define data storage patterns and policies from a single console. Especially valuable for sensitive and regulated data, this engine delivers actionable intelligence that supports more informed decisions about storage optimization, regulatory compliance, and data governance and security.

☒ **INFORMATION MAP:** Enables data visibility in a fragmented IT ecosystem. Information Map is a data visualization tool that gives IT a comprehensive view of structured and unstructured data, what data should be protected, what shouldn't and where agencies can save by moving to lower-cost storage.

☒ **DATA INSIGHT:** Provides analytics, reporting and tracking for data use and security for organizations that manage enormous amounts of data. Data Insight also integrates with archiving and security platforms to prevent data loss, drive cost savings and compliance, and improve overall information governance.

Phase 2: MANAGE

> **“The best way to improve data management is to have a proper governance and compliance program in place. You also need to address these requirements up front, before you start to unlock the potential of data and its uses.”**
>
> — Michael Sherwood, Director of Innovation and Technology, Las Vegas

Government agencies may store unnecessary data. Much of this information has no value anymore — it just increases the agency’s costs for storage systems and backup resources.

To manage data effectively, government IT teams need to understand what data they have and where it is stored. They also need systems that are designed to adapt easily to meet increasing and diverse regulatory mandates for data privacy, retention schedules and deletion. But perhaps most importantly, IT needs an active strategy for data governance — managing data in a way that maintains compliance while serving agency needs.

CREATING STRONG DATA GOVERNANCE PRACTICES

A robust data governance program positions IT to comply with new regulations quickly and easily, and improve data management overall. Formal governance practices also help IT teams better understand the agency’s data, improve how it is stored and accessed, and identify ways it can better serve all stakeholders.

“The best way to improve data management is to have a proper governance and compliance program in place,” says Sherwood. “You also need to address these requirements up front, before you start to unlock the potential of data and its uses.”

A strong data governance and management program is built upon two things: The work of a governance committee and governance processes that are automated with technology. A governance committee typically includes representatives from IT, legal, records management, human resources, and business or program groups within the agency. To achieve success, the committee and its policies should have the support of agency executives.

After the committee has established core governance policies, IT can use technology to automate data monitoring, auditing, management and policy enforcement processes. Automated governance processes help agencies keep data under proper control, especially when budgets are tight. Additionally, automated data retention and deletion help agencies show compliance in a way that has stronger credibility than manual processes.

HOW TECHNOLOGY HELPS DATA GOVERNANCE

"Government IT teams need systems that can help them easily plan governance, adapt to changes in compliance requirements and manage data on a budget," says Darryl Richardson, senior systems engineer for Veritas.

Solutions to consider for data management and governance focus on three critical dimensions: visibility, retention and discovery.

Visibility tools provide insight into key attributes of each data asset such as metadata information, true ownership, categorization and disposition.

Retention tools help IT identify the best choices for long-term data storage based on details about the asset's content, ownership and usage.

Electronic data discovery tools help government teams quickly respond to public records requests and court orders, and comply with legal discover requirements on a repeatable and reportable basis.

COMPREHENSIVE DATA MANAGEMENT SOLUTIONS

Improving data management and governance requires a blend of practices and technologies. Veritas helps agencies achieve this blend with solutions that enhance data visibility, access, retention and discovery.

- **ACCESS:** Uses intelligent policies to optimize data placement in on-premises or public cloud storage. As a solution for software-defined storage, Access helps IT meet performance needs for unstructured data, manage data based on policy, seamlessly move data to and from multi-cloud platforms, and obtain cost-effective, long-term data protection and archiving.

- **INTEGRATED COGNITIVE OBJECT STORAGE:** Enables innovative applications by orchestrating, processing and taking action on data as it is received. This solution allows for deeper inspection and classification of data to help ensure sensitive information is properly managed and protected.

- **ENTERPRISE VAULT:** Helps agencies simplify and reduce the cost of information retention, management and discovery. Based on each organization's requirements and needs, Enterprise Vault scans applications and automatically migrates information to an archive to improve regulatory compliance.

- **ENTERPRISE VAULT CLOUD:** Interfaces seamlessly with cloud-based office application suites and on-premises email systems to ensure proper information retention. As a cloud-based archiving service, this solution helps agencies more effectively meet data governance requirements and more efficiently execute business or legal eDiscovery processes.

- **eDISCOVERY PLATFORM AND COMPLIANCE ACCELERATOR:** Helps agencies isolate relevant information they need to access. This solution allows agencies to better control their data and generate insights that improve service delivery and reduce the costs of storage, backup and server maintenance.

Phase 3: SECURE

Government data is an attractive target for cybercriminals. The potential for a breach that would impact citizens, impair government operations and damage public trust has made secure data management a top IT priority for state and local government agencies. However, several challenges may hinder an agency's security measures.

The first challenge comes with moving data to the cloud. Although a cloud provider may meet all security requirements, an agency still has the responsibility to identify which data is appropriate for cloud storage and to set up the right governance policies and procedures.

The second challenge comes with online service portals for citizens. IT needs technology that protects citizen privacy while also preventing someone from using the portal as an entryway for unauthorized access to other sensitive data or applications.

Finally, because IT staffs are often stretched thin, application patching isn't always done in a timely manner. When patch processes aren't automated, data and applications are vulnerable to a breach or ransomware attack.

Several strategies can help agencies address these

WHEN PATCH PROCESSES AREN'T AUTOMATED, DATA AND APPLICATIONS ARE VULNERABLE TO A BREACH OR RANSOMWARE ATTACK.

security challenges and improve data protections.

An initial strategy is to implement continuous security monitoring across the IT infrastructure. This helps identify easy-to-fix issues such as needed application patches or users who haven't updated passwords.

The next step is to consider adopting the cybersecurity framework published by the National Institute of Standards and Technology (NIST) or the Defense Information Systems Agency (DISA). These frameworks offer a comprehensive view into security best practices across IT systems and applications as well as the enterprise network and cloud services.

Many public sector organizations have already adopted one of these frameworks as a tool to improve their security programs.

SOLUTIONS FOR A STRONG SECURITY FOUNDATION

Any cybersecurity program is only as strong as its foundation. A standards-based framework is essential, as are strong security technologies. Veritas offers a unified approach to keep data and applications safe, both on-premises and in the cloud.

☒ **CLOUDPOINT:** Provides a single, central dashboard to consistently manage backup and recovery for all data across an environment of multiple public and private clouds. CloudPoint also alleviates risk and compliance concerns with automated discovery of new cloud instances and applications for backup in seconds.

☒ **RESILIENCY PLATFORM:** Enables agencies to manage different information environments using a single, automated solution. The platform offers a unified approach to improve the predictability and resiliency of an organization's entire IT ecosystem, with:

- Visibility and tracking of recovery time objectives and recovery point objectives from a single, web-based dashboard
- The ability to move workloads between on-premises data centers and the cloud or between clouds in a single click
- Simple integrations as the IT environment changes
- Compliance tools that enable audit reporting and the ability to test new features without service disruptions

Detailed frameworks help an agency assess its current security measures and identify needed changes in areas such as risk management, internal security operations and threat response.

Internal education is also a key strategy when evaluating the security of potential cloud solutions. Klimek recommends involving system administrators, legal staff, and the networking and security teams.

"Everybody needs to have input into the decision because it impacts them differently from how it impacts your IT team. All potential security and operational ramifications need to be reviewed and addressed so you can get buy-in from everyone," he says.

Sherwood adds that agencies need to focus on protecting data integrity. "When you protect data from tampering, this focus will naturally lead you to implement good security measures," he says.

RIGOROUS SECURITY WITH DATA STORAGE TECHNOLOGY

"Designing storage in a way that separates the data and content from online applications and servers is a key measure to protect against a data breach," says Sabre Schnitzer, manager of compliance for Veritas Public Sector. This storage system design encompasses four key elements.

1. **A standards-based framework:** Choose storage products based on NIST and DISA standards.
2. **Automated updates:** Implement storage solutions that support automated processes for applying software updates and security patches.

> **"Designing storage in a way that separates the data and content from online applications and servers is a key measure to protect against a data breach."**
>
> — Sabre Schnitzer, Manager of Compliance, Veritas Public Sector

3. **Vendor security measures:** Verify the vendor has a sound process to identify security vulnerabilities that emerge during product development. Also compare vendor response times for remediating product vulnerabilities reported by customers and third-party evaluators.
4. **Cloud services monitoring:** Maintain processes to monitor the security of the vendor's cloud services and govern user access to data stored in the cloud.

CONCLUSION

"Data has become an essential public service, like water or public safety," says Sherwood. "Data is more important than ever to bring new types of economic opportunities to a community as well as better decision-making and greater efficiency within a government."

This perspective reflects both the potential and the challenge presented by data. State and local government IT teams must store and manage growing volumes of data in both on-premises systems and the cloud. This data must be readily accessible to help employees work efficiently and meet constituent expectations for responsive services. And the data must be managed in a way that complies with myriad regulatory and privacy requirements.

Good strategies for data design, management and security are about more than just coping with growing data volumes. The strategies presented in this handbook will help governments improve the availability and use of that data for internal operations and public services for years to come.

ENDNOTES

1. http://www.govtech.com/library/papers/Big-Data-or-Big-Hype-99664.html?promo_code=GOVTECH_web_library_list
2. Ibid.
3. 2018 Center for Digital Government data analytics survey of 116 state and local government officials.

PRODUCED BY:

CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com**

FOR:

VERITAS

Veritas Technologies enables organizations to harness the power of their information to drive business success, with solutions designed to serve the world's most complex, heterogeneous environments. Veritas works with state and local governments to help them improve data availability and unlock insights into their data to reduce risk and increase compliance.

From traditional data centers to private, public, and hybrid clouds, Veritas helps organizations protect, identify, and manage data regardless of their environment. Veritas' products for backup and recovery, business continuity, software-defined storage, and information governance help automate information management so organizations can focus on enhancing the citizen experience. **https://www.veritas.com/**

carahsoft

Carahsoft Technology Corp. is the trusted Government IT solutions provider, supporting an ecosystem of manufacturers, value-added resellers, system integrators, and consulting partners committed to helping government agencies select and implement the best solution at the best value.
The company's dedicated Solutions Divisions proactively market, sell and deliver VMware, Symantec, Veritas, Adobe, F5 Networks, Open Source, HPE Software, SAP, and Innovative and Intelligence products and services, among others. Carahsoft is consistently recognized by its partners as a top revenue producer, and is listed annually among the industry's fastest growing firms by CRN, Inc., Washington Technology, The Washington Post, and Washington Business Journal. **www.carahsoft.com**

UNLESS NOTED ALL PHOTOS PROVIDED BY SHUTTERSTOCK.COM