HURON

What every nonprofit’s data protection solution should include

By Mike Melone and John Vega

As nonprofit organizations seek to enhance constituent engagement, increase revenue, and streamline operations, customer relationship management (CRM) systems are becoming an ever-vital component of their technology landscape. CRM systems like Salesforce enable organizations to deliver targeted, consistent touch points, maximize fundraising potential, and automate business workflows. Your CRM is only as good as what you put in it though, so it’s critical to ensure that data is readily available and secure. Yet, a deliberate plan to protect and safeguard data is an often-overlooked aspect of technology investments, especially for nonprofit organizations.

In Brief

- Nonprofits need to prioritize data protection to maintain business continuity and safeguard constituent data.
- A multi-prong approach to data protection should include backup and recovery, data archiving, data classification, and encryption.
- Strategies for data backup and recovery should prioritize automation, off-premises storage, testing, and quick and full restoration.

Nonprofit cybersecurity numbers tell a consistent story. Only 20% of nonprofits have a policy in place to address cyberattacks, and only 26% are actively monitoring their networks for data losses and breaches. Seventy percent of nonprofits have never run a data vulnerability assessment to evaluate potential risk exposure. Thus, it should come as no surprise that, over the last year, nonprofits were responsible for more than two million data incidents.

The most powerful tool an organization has to manage constituents is data. Nonprofits with well-developed data protection policies are better positioned to weather unexpected data loss incidents without dramatically impacting their business. To maintain business continuity, manage data volumes, and ensure data privacy, organizations need a complete, multi-prong approach to successfully manage their data with focus areas that include backup and recovery, data archiving, data classification, and encryption.

Data backup and recovery

First and foremost, organizations are responsible for and need to protect against data loss. Studies show that most data loss incidents result from user error rather than external factors. As such, data backups that you can readily restore enable organizations to safeguard against unforeseen data losses, which are more common than most people realize.

When establishing a backup and recovery strategy, nonprofits should consider the following:

- **Implement an automated backup solution.** Dependency on manual processes can lead to inconsistency in backup collection and practices. Human involvement is best suited to the creation of the program and data restoration.
- **Store backups outside of production systems.** A common safeguard for data loss protection is to store backup data in other locations from its original source. Off-premises locations, not subject to an organization's technology infrastructure, are highly encouraged for added protection. This is a good use case for cloud services that store, protect, and enable easy data restoration.
- **Test backups.** Many organizations that regularly perform backups do not test a data restore. While these processes can be straightforward, depending on the tool being used, restoring data for the first time during a data loss incident can add stress and be prone to further incidents due to executing an unfamiliar process.
- **Restore quickly and fully.** Ensure your backup and recovery solution has tools to proactively monitor application data and quickly alert you to unusual data loss or corruption. It should also provide an analysis of the extent and timing of loss or corruption and allow you to restore specific records.

Data archive

As organizations' systems grow, data volume can become a concern. Large data volumes can often lead to system performance and reporting challenges.

The nonprofit industry is no stranger to large data concerns with ever-increasing pools of constituent data. As a result, organizations need to think through their data retention policy proactively, archive records to maintain reasonable data volumes, and develop strategies to access archived records or summary data in integrated systems if needed.

When establishing a data archive strategy, nonprofits should consider the following:

- **Develop a clear data retention policy.** A clearly documented data retention policy enables an effective data purge and archiving practice. A data retention policy also supports compliance with various regulations that dictate how long you should keep certain types of data. With clear expectations, these practices can be automated, creating greater operational effectiveness and efficiency.
- **Understand the implications of related data objects.** Most CRM systems have parent-child records that need to be fully understood for an archiving strategy to ensure data integrity. Otherwise, an organization risks creating orphan records that can lead to user interface confusion, stakeholder loss of confidence, and lack of user adoption.
- **Know if archived data needs to be accessible.** To ensure system performance, organizations may need to archive data that hasn't been viewed for a while but still needs to be accessible to users. For example, a donor services team may need to view gifts made several years ago to support donor inquiries. As a result, organizations need a clear strategy for handling these situations. Will staff be expected to access more than one system? Or is the organization prepared to create views into archived data within its CRM system, such as in the case of the Salesforce platform that enables API views directly from page layouts?

One important point to remember is that data backups are not meant to serve as a data archive strategy. Backups protect against data loss by capturing current records to restore if needed. An archive is collected historical data removed from an organization's source system and stored elsewhere for reference as needed.

Data classification and encryption

Given nonprofits' numerous interactions with their constituents, organizations are likely to have a range of data with varying degrees of sensitivity. In addition to backing up and archiving data, organizations need to comprehend the sensitivity of their data and develop a framework to manage associated risks.

Examples of sensitive data nonprofits may have are personal identifiable information (PII), financial information, and health and welfare data. As cyber theft becomes an increased threat to organizations, nonprofits need to safeguard their data. Organizations that cannot meet this baseline competency in the digital economy run the risk of being poor stewards of constituent data and eroding trust among supporters.

When establishing a data classification and encryption strategy, nonprofits should consider the following:

- **Classify your data.** Organizations first need to create an inventory of housed data and classify them into varying sensitivity levels. With this completed inventory, a nonprofit can evaluate its compliance with legal and regulatory requirements and industry best practices. These initial tasks are critical to identifying an organization's risk point. While this work may seem straightforward, it can be lengthy, tedious, and risky. Given the high visibility and risk involved with a potential data breach, organizations would be wise to consider vendor partners in this work.
- **Develop a data encryption plan.** One of the most effective methods for protecting data is encryption. The ability to encrypt data not only in transit but at rest as well is an important capability in an organization's toolset to protect data. That said, there are different methods for at-rest encryption, and nonprofits need to be clear on what solution works best for their business processes. Choosing an encryption practice that does not align with business operations can result in additional, unnecessary complexity and impact system performance. This is another case in which organizations may want to engage with a trusted partner to ensure the best possible decisions are made.

Secure systems without impacting operations

Data protection is essential for nonprofit organizations to ensure business continuity and protect the privacy of their constituents. A comprehensive data protection approach should include backup and recovery, archiving, classification, and encryption processes.

By implementing these strategies, nonprofits can better secure their systems without significantly impacting their operations. With the right plan in place, organizations can rest assured that all their constituent data will remain secure as they grow their mission-driven work.

HURON

huronconsultinggroup.com