VITAL CYBER
Provided by MCNC

Episode 4: Data Management

Question about a term?
Visit our Glossary

Did you know that it's believed that over 80% of data breaches involve unstructured data? Welcome back to "Cybersecurity 101: Securing Your Digital Environment," where today, we're diving into the cornerstone of cybersecurity—Data Management (DM). Think of DM as the glue holding your security framework together. Overlooking it can result in breaches, compliance problems, and the loss of critical information. Mastering DM isn't just a recommendation—it's essential for safeguarding your organization's most valuable asset, its data.

How Do You Manage Data?

So, how do you manage data, and why is it crucial for your organization? You may recall that we defined an asset as anything useful or valuable to the organization. In the context of data, this includes everything from customer information and financial records to intellectual property and operational metrics. Whether it's stored in cloud services, on local servers, or even in employee devices, all of this data is part of your organization's inventory.

Managing data involves overseeing its entire lifecycle, from collection and storage to usage, updates, and, ultimately, secure disposal. It's more than just keeping track of where your data is stored—it's about documenting key metadata, including ownership, classification, retention requirements, and access controls. This structured approach helps protect sensitive information and ensures that your organization complies with regulatory requirements and can quickly respond to data-related incidents or audits.

The Framework

Before beginning to build out your DM program, take a moment to review the key safeguards outlined in the CIS Version 8.1 framework. These safeguards provide a clear roadmap for securing and managing your data effectively. Let's break them down to help you build a strong foundation for your DM strategy:

- **Basic Cyber Hygiene (IG1).**
    - (CIS 3.1)Establish and Maintain a Data Management Process
    - (CIS 3.2)Establish and Maintain a Data Inventory
    - (CIS 3.3)Configure Data Access Control Lists
    - (CIS 3.4)Enforce Data Retention
    - (CIS 3.5)Securely Dispose of Data
    - (CIS 3.6)Encrypt Data on End-User Devices
- **Additional Safeguards (IG2).**
    - (CIS 3.7) Establish and Maintain a Data Classification Scheme
    - (CIS 3.8) Document Data Flows
    - (CIS 3.9) Encrypt Data on Removable Media
    - (CIS 3.10) Encrypt Sensitive Data in Transit
    - (CIS 3.11) Encrypt Sensitive Data at Rest
    - (CIS 3.12) Segment Data Processing and Storage Based on Sensitivity

Where To Start?

To get started with DM, establish clear administrative controls that outline fundamental safeguards for data protection and any additional measures needed to address your organization's specific needs.

- **Policy**: The first step is developing a DM policy that defines roles and responsibilities, including who oversees your DM process, how data assets are inventoried and classified, and the actions to be taken during each data lifecycle phase. A well-defined policy provides a framework for consistent and effective DM process across the organization. To get started, consider using our template, which includes the essential elements of a DM policy.
- **Standards and Procedures**: Once the policy is in place, establish detailed standards and procedures to translate the policy into actionable, daily practices. These documents serve as a practical guide for data classification, protection, and disposal tasks, ensuring everyone involved in managing data understands their responsibilities. Check out our templates for standards and procedures that cover the essentials and can be tailored to fit your organization's needs.

Where Do We Go From Here?

Now that you've established your administrative controls, it's time to implement them by documenting and managing your data assets through each phase of their lifecycle.

- **Acquisition**: Verify that received data comes from trusted, authorized sources. For example, ensure customer data is obtained via secure channels that comply with privacy regulations like GDPR or HIPAA. Properly document each new data asset, detailing its source, ownership, and intended use.
- **Inventory**: Maintain an inventory of your data assets, including their location, ownership, and classification. You should start by inventorying sensitive data. You can use automated tools or spreadsheets; here's a template to track and update the inventory.
- **Classification**: Assign each data asset a sensitivity and criticality level to determine the appropriate protection measures. Clear classification ensures data is handled by its value and risk.
- **Protection**: Implement safeguards such as encryption, access controls, and monitoring to secure data against unauthorized access or breaches. Update your inventory with the protective measures applied to each asset.
- **Handling**: Ensure data is stored, accessed, and shared securely throughout its lifecycle. Regularly review handling practices to align with organizational policies and regulatory requirements.
- **Disposal**: Securely delete or destroy data no longer needed to prevent unauthorized recovery or misuse. Update your inventory to reflect the removal of data assets.

Securing your organization's data doesn't have to be intimidating. By following these lifecycle steps, you'll be well on your way to a safer, more efficient data management process.

Where We're At!

Building upon the Cybersecurity Framework in episode one, here is a visualization of the progress made to this point in the series. We recommend you copy this sheet or create your own to visualize your progress.

Take the Next Step in Strengthening Your Cybersecurity

Is your organization ready to enhance its cybersecurity posture? Our team of experts at MCNC is here to help. Whether you need a comprehensive risk assessment, policy analysis, or guidance on implementing best practices, we're ready to partner with you to safeguard your digital assets.

Don't wait until it's too late. Contact us today to schedule a consultation and discover how MCNC's Vital Cyber solutions can protect your institution. Fill out our Contact Us form and let's start building a stronger defense together.