O'HAGAN MEYER

RAPID RESPONSE & INCIDENT MANAGEMENT

Data Retention Best Practices

Businesses collect various types of data from different sources. It is important to consider how to properly manage and store that data to limit potential harm to your business and its customers. The following data retention best practices can help when considering a data retention policy.

Identify your data: The first step in determining your data retention policy is to identify the data you have in your possession. You must undertake a comprehensive review of all of the data that your company holds, identify the various types of data, identify the source of the data, and identify where the data resides on your system. Once you have properly identified and classified your data, you establish an appropriate data retention policy.

Identify applicable laws and regulations: Different laws and regulations will apply to your organization depending on the types of data that are in your possession. For example, if you collect data from children under 13 years of age, the Children's Oline Privacy Protection Act requires that you only retain this information for as long as necessary to fulfill the business purpose for which it was collected, while under the Gramm-Leach-Bliley Act, financial institutions must dispose of customer information no later than two years after the last date the information was used, unless retention is otherwise required or necessary for a legitimate business purpose. It is important to identify which data retention regulations apply to the types of data in your possession.

Create a written data retention policy: Your data retention policy should be documented in writing and available to all of your employees. The policy must be readily available to ensure that all employees are familiar with the policy. The policy should include information regarding the security of the information as well as the proper destruction of the information. The policy should also identify the individuals in your organization responsible for enforcing the policy.

Employee Training: Data retention information should be part of the regular cybersecurity training for your employees. This will ensure that your employees are familiar with the policy and also understand the importance of the policy. All employee training should be mandatory and should be documented.

Limit Access: Access to information should be limited to those employees that need access to perform their job responsibilities. Limiting access reduces the potential for the unauthorized disclosure of information, either by accident or through an attack on your computer system.

Do not hold data longer than is necessary: Data should be purged from your system, either as required by law, or once that data no longer has a business purpose. Holding data longer than is necessary creates an unnecessary risk that the data will be compromised. Once data no longer serves a business purposes, it should be deleted.