

DATA CLASSIFICATION PRACTICES: FACILITATING DATA-CENTRIC SECURITY MANAGEMENT

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of implementing data-centric security management through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Data Classification Practices: Facilitating Data-Centric Security Management project, including background, challenges, and goals.

BACKGROUND

A critical factor for achieving success in any organization is the ability to share information and collaborate effectively and efficiently while satisfying the security and privacy requirements for protecting that information. Conventional network-centric security measures are increasingly ineffective for protecting information as systems become more dispersed, mobile, dynamic, and shared across different environments and subject to different types of stewardship. As part of a zero trust approach, data-centric security management aims to enhance protection of information (data) regardless of where the data resides or who it is shared with.

Data-centric security management necessarily depends on organizations knowing what data they have, what its characteristics are, and what security and privacy requirements it needs to meet so the necessary protections can be achieved. Standardized mechanisms for communicating data characteristics and protection requirements are needed to make data-centric security management feasible at scale.

CHALLENGES

- The limited nature of existing standards for data classifications means that most organizations do not use classifications that are consistent with those of their partners and suppliers.
- The lack of common definitions for classifiers can result in information being classified and labeled inconsistently.
- The distributed nature of data can complicate the process of establishing and maintaining data inventories.
- Data classifications and data handling requirements often change during the data lifecycle, requiring the capability to adjust to those changing requirements.

GOAL

The goal of this project is to recommend technology-agnostic practices for defining data classifications and data handling rulesets and for communicating them to others. This project will inform, and may identify opportunities to improve, existing cybersecurity and privacy risk management processes by helping with communicating data classifications and data handling rule sets. It will not replace current risk management practices, laws, regulations, or mandates.

DOWNLOAD PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the project. To learn more, download the project description at: www.nccoe.nist.gov/data-classification.



HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have a question about this project or would like to join the Data Classification Community of Interest, please email data-nccoe@nist.gov.