NIST SPECIAL PUBLICATION 1800-28A

Data Confidentiality:

Identifying and Protecting Assets Against Data Breaches

Volume A:
Executive Summary

William Fisher
National Cybersecurity Center of Excellence
NIST

R. Eugene Craft
Michael Ekstrom
Julian Sexton
John Sweetnam
The MITRE Corporation
McLean, Virginia

December 2023

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/data-confidentiality-identifying-and-protecting-assets-against-data-breaches

Executive Summary

CHALLENGE

In our data-driven world, organizations must prioritize cybersecurity as part of their business risk management strategy. Specifically, data security remains a challenge as attacks against an organization's data can compromise emails, employee records, financial records, and customer information thereby impacting business operations, revenue, and reputation. In the event of a data breach, data confidentiality can be compromised via unauthorized exfiltration, leaking, or spills of data or corporate information to unauthorized parties, including the general public. This can be intentional or accidental.

In the event of an ongoing data breach, it is essential that an organization be able to detect the ongoing breach themselves, as well as begin to execute a response and recovery plan that leverages security technology and controls.

BENEFITS

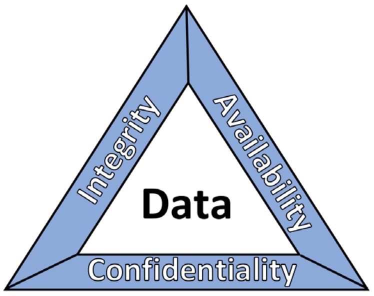
The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) developed this guide to help organizations implement strategies for preventing recovering from data confidentiality attacks. This NIST NCCoE Cybersecurity Practice Guide demonstrates how organizations can develop and implement appropriate actions to identify and protect data against a confidentiality cybersecurity event. It includes numerous technology and security recommendations to improve your organization's cybersecurity posture.

This practice guide can help your organization:

- Identify data on your network that is vulnerable to a data breach
- Identify vulnerabilities to data breaches on your network
- Implement protective technologies to prevent data breaches

APPROACH

This is part of a series of projects that seek to provide guidance to improve an organization's data security in the context of the CIA triad. The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability. This practice guide focuses on **data confidentiality**: the property that data has not been disclosed in an unauthorized fashion. Data confidentiality concerns data in storage, during processing, and while in transit. (Note: These definitions are from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12 Rev 1, *An Introduction to Information Security*.)



This guide applies data confidentiality principles through the lens of the NIST Cybersecurity Framework version 1.1. Specifically, this practice guide informs organizations of how to **identify** and **protect** assets, including data, against a data confidentiality attack, and in turn understand how to manage data confidentiality risks and implement the appropriate safeguards. A complementary project and accompanying practice guide (SP1800-29) addresses data confidentiality through the lens of detecting, responding, and recovering from a data confidentiality attack.

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
FRAMEWORK

The NCCoE developed and implemented a solution that incorporates multiple systems working in concert to identify and protect assets and data against detected data confidentiality cybersecurity events. The solution will demonstrate the ability to identify assets and data that are at risk of a data breach and recommend capabilities to help protect them.

In developing this solution, the NCCoE sought existing technologies that provided the following capabilities:

- **Logging**
- **Network protection**
- **User access control**
- **Data management**
- **Data protection**
- **Policy enforcement**
- **Browser isolation**

Collaborator	Security Capability or Component
Avrio Software (now known as Aerstone)	Data Management
Cisco	Policy Enforcement, User Access Control
Dispel	Network Protection
FireEye	Logging
PKWARE	Data Protection
Qcor	Data Protection
Strongkey	Data Protection
Symantec, a Division of Broadcom	Browser Isolation

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-28a: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-28b: Approach, Architecture, and Security Characteristics,* which describes what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-28c: How-To Guides*, which provide specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/data-security/dc-detect-identify-protect. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at ds-nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.