NIST SPECIAL PUBLICATION 1800-25A

Data Integrity:

Identifying and Protecting Assets Against Ransomware and Other Destructive Events

Volume A:
Executive Summary

Jennifer Cawthra
National Cybersecurity Center of Excellence
NIST

Michael Ekstrom
Lauren Lusty
Julian Sexton
John Sweetnam
Anne Townsend
The MITRE Corporation
McLean, Virginia

December 2020

FINAL

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-25.

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect.

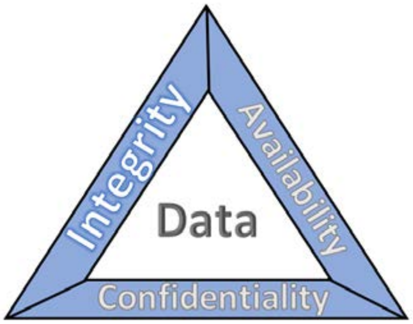
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Executive Summary

The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability, as follows:

- Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity — guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity
- Availability – ensuring timely and reliable access to and use of information



This series of practice guides focuses on data integrity: the property that data has not been altered in an unauthorized manner. Data integrity covers 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*.)

- Destructive malware, ransomware, malicious insider activity, and even honest mistakes all set the stage for why organizations need to properly identify and protect against events that impact data integrity. Businesses must be confident that data is protected and safe.
- Attacks against an organization's data can compromise emails, employee records, financial records, and customer information—impacting business operations, revenue, and reputation.
- Examples of data integrity attacks include unauthorized insertion, deletion, or modification of data to corporate information such as emails, employee records, financial records, and customer data.
- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore methods to effectively identify and protect against data integrity attacks in various information technology (IT) enterprise environments to prevent impacts to business operations.
- This NIST Cybersecurity Practice Guide demonstrates how organizations can develop and implement appropriate actions before a detected data integrity cybersecurity event.

IDENTIFY
PROTECT
CYBERSECURITY
FRAMEWORK
VERSION 1.1

CHALLENGE

Some organizations have experienced systemic attacks that force operations to cease. One variant of a data integrity attack–ransomware–encrypts data, rendering it unusable. This type of impact to data affects business operations and often leads them to shut down. Other variants of data integrity attacks can steer organizations to make decisions that can impact the bottom line or execute ill-fated decisions.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-25.

For example, adversarial actors could create backdoor accounts in company login systems, change payroll information to their benefit, or expose the company with unsafe software updates for their own benefit.

SOLUTION

NIST published version 1.1 of the Cybersecurity Framework in April 2018 to help organizations better manage and reduce cybersecurity risk to critical infrastructure and other sectors. The framework core contains five functions, listed below.

- **Identify** – develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
- **Protect** – develop and implement appropriate safeguards to ensure delivery of critical services
- **Detect** – develop and implement appropriate activities to identify the occurrence of a cybersecurity event
- **Respond** – develop and implement appropriate activities to take action regarding a detected cybersecurity incident
- **Recover** – develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

RECOVER
IDENTIFY
CYBERSECURITY FRAMEWORK VERSION 1.1
RESPOND
PROTECT
DETECT

For more information, see the *Framework for Improving Critical Infrastructure Cybersecurity*.

Applying the Cybersecurity Framework to data integrity, this practice guide informs organizations of how to identify and protect assets against a data integrity attack, and in turn understand how to manage data integrity risks and implement the appropriate safeguards.

The NCCoE developed and implemented a solution that incorporates multiple systems working in concert to identify and protect assets against detected data integrity cybersecurity events. The solution isolates the opportunities that would allow for the cybersecurity events to occur and implements strategies to remediate the opportunities. Also, the solution applies additional protections from cybersecurity events to IT infrastructure.

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

- **inventory**
- **policy enforcement**
- **logging**
- **backups**
- **vulnerability management**

- **secure storage**
- **integrity monitoring**

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.

BENEFITS

This practice guide can help your organization:

- develop a strategy for identifying and protecting assets against a data integrity cybersecurity event
- facilitate comprehensive protection from adverse events to maintain operations and ensure the integrity of data critical to supporting business operations and revenue-generating activities
- manage enterprise risk (consistent with foundations of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*)

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/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.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations 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). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

CISCO CRYPTONITE NXT GreenTec www.GreenTec-USA.com MICRO FOCUS SEMPERIS Symantec. tripwire

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.

LEARN MORE
Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200