PROJECT DESCRIPTION

DATA CONFIDENTIALITY

Identifying and Protecting Assets and Data Against Data Breaches

Jennifer Cawthra

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Michael Ekstrom
Lauren Lusty
Julian Sexton
John Sweetnam
Anne Townsend

The MITRE Corporation

December 2019

ds-nccoe@nist.gov

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a Community of Interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

ABSTRACT

An organization must protect its information from unauthorized access and disclosure. Data breaches large and small can have far-reaching operational, financial, and reputational impacts. The goal of this project is to provide a practical solution to identify and protect the confidentiality of an enterprise's data. This solution identifies what assets (devices, data, and applications) may be affected by an incident as well as the vulnerabilities they may possess that allow incidents to occur. It also explores protection measures to mitigate or remediate these vulnerabilities. The solution will provide measures such as data protection, access controls, network protections, and other potential defenses. The project team will create a reference design and a detailed description of the practical steps needed to implement a secure solution based on standards and best practices. This project will result in a freely available NIST Cybersecurity Practice Guide.

KEYWORDS

data breach; data confidentiality; data loss; data protection; malware; ransomware; spear phishing

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Purpose

This document defines a National Cybersecurity Center of Excellence (NCCoE) project to provide guidance and a reference architecture that will assist organizations in identifying and protecting information from threats to data confidentiality. Data confidentiality refers to the protection of data from unauthorized access and disclosure, including means for protecting personal privacy and proprietary information. Confidentiality is relevant for data at rest, in use, and in transit. Lapses in data confidentiality can lead to a data breach. A breach may include internal and external unauthorized access or disclosure. According to the 2018 Cost of Data Breach Study conducted by Ponemon Institute and sponsored by International Business Machines [1], the worldwide average cost of a data breach in 2018 was $3.55 million.

NCCoE projects include technical guidance and a reference architecture that address a technical challenge. An example implementation of the reference architecture integrates commercial and open-source products to demonstrate how to incorporate standards and best practices. This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

Scope

This project will answer specific questions pertaining to identifying and protecting data from data confidentiality attacks, such as:

- What data is present within an enterprise?
- What protections can be applied to the data?
- How should the data be accessed?
- What user types are defined by the organization?
- What controls should be applied to each user type's access?

This project will demonstrate:

- a data management solution that identifies and inventories data on and across end points
- a solution that provides user access control mechanisms
- a solution that protects against malicious physical media
- a policy enforcement solution that manages users and user access controls
- an audit log solution that baselines normal behavior for data access activity and protects against exfiltration
- a file level encryption scheme that protects data on and across end points
- a system level encryption scheme that provides physical access protection
- network measures to protect data in transit

This project will not address data security issues related to integrity or availability. This includes violations of machine integrity that can lead to the loss of data confidentiality, such as a compromised Active Directory server that allows unauthorized access to network machines. For more information about issues of data integrity, please see the Data Integrity series of the data security projects, found at https://www.nccoe.nist.gov/projects/building-blocks/data-security. Questions of data classification, such as what data is at risk and requires greater protection, will

not be covered. For more information, please refer to the Implementation Decisions section below.

Assumptions/Challenges

Protecting Against the Privileged Insider

The privileged insider who causes data confidentiality incidents, whether accidentally or intentionally, is difficult to prevent. Preemptive measures can be taken to ensure that the impact of a malicious insider is recorded and mitigated. Training can be given to these users to minimize the risk of unintentional events. However, some risk will always remain. Activity concerning privileged insiders will be addressed in the project's use cases, but organizations should be aware of the limitations of technical solutions surrounding these scenarios.

Implementation Decisions

There is a trade-off between the strength of protections on data and the time and resources spent maintaining those protections. An organization should make risk-based decisions as to what data should be considered sensitive for the organization and what warrants extra protections. This project will assume that organizations can identify their at-risk data and tune the final reference architecture to reflect their risk management policy. The reference architecture will aim to include tools that will allow organizations to classify data as sensitive and at risk. However, we will not be able to provide guidance as to what data should be considered sensitive and what should be considered at risk.

Cloud Versus On-Premises

While the overarching principles of identifying and protecting data confidentiality are infrastructure-agnostic, the implementations of those principles are not. More businesses are turning to cloud-based solutions to provide enterprise function, modularity, security, and more. While the Data Confidentiality Project will primarily use an on-premises infrastructure, the final guidance provides references to the NCCoE's cloud security work where applicable. This will aid adopters in adapting the guidance to enterprise implementation that uses on-premises, cloud, or both. For more information about the NCCoE's current work in cloud, please see https://nccoe.nist.gov.

Background

The first group of data security projects at the NCCoE focused on data integrity (DI). The NIST Special Publications covered the ability to protect DI, detect and respond to attacks that impact DI, and recover DI after an attack [2]. During presentations, demonstrations, Community of Interest calls, and other feedback mechanisms, many questions were raised related to data breaches and inclusion of technologies to prevent such attacks. These attacks (and therefore incorporation of their mitigating technologies) were outside the scope of the DI projects because they were not addressing DI events; thus, they were categorized as data confidentiality challenges.

In addition to the work focused on data integrity, the NCCoE engaged with consumer-facing and retail organizations and e-commerce payment stakeholders such as information sharing and analysis centers and the Retail Cyber Intelligence Sharing Center (now known as the Retail and Hospitality Intelligence Sharing and Analysis Center). Through these engagements, the need for data confidentiality projects was identified.

This project will provide guidance on data confidentiality together with the Detect, Respond to, and Recover from Data Breaches Project. The NCCoE chose to address data confidentiality in

two parallel projects to provide modular, adaptable guidance rather than an all-or-nothing approach. In addition, two projects allow multiple perspectives into scenarios for preventing and reacting to a data breach or other loss of data confidentiality. In summary, securing a system by identifying and protecting against threats requires technologies, planning, and training that are different from detecting, responding to, and recovering from a breach.

2 SCENARIOS

The example scenarios below illustrate some of the challenges that this project will address.

Scenario 1: Exfiltration of Encrypted Data

An organization unknowingly has a compromised machine that is being used by a malicious actor to exfiltrate data. The malicious actor is encrypting the data to prevent detection.

The data confidentiality solution will identify the data and where it is stored before the compromise and apply the appropriate controls. Furthermore, the architecture should serve to protect sensitive data in storage and in transit.

Scenario 2: Spear Phishing Campaign

As a result of a spear phishing campaign, a malicious actor can view and manipulate a database. Proprietary internal data stored in the database is exposed.

The data confidentiality solution will protect the database from unauthorized access as well as protect the data in the database, which will mitigate the effects of a breach.

Scenario 3: Ransomware

An employee is a victim of ransomware and is presented with a note showing contents of the proprietary files from the employee's organization's file server and a demand for money to stop accessing and sharing files.

The data confidentiality solution will protect the file share from unauthorized access as well as protect the data in the file share and network connectivity.

Scenario 4: Accidental Email

A user accidentally cc's an individual who should not have access to the email's attachment, which contains proprietary information. The cc'd individual could be either an employee or an outsider to the organization.

The data confidentiality solution will identify the files, protect the files from unauthorized access, and provide email protections to prevent the accidental inclusion.

Scenario 5: Lost Laptop

A user loses their laptop that contains proprietary company information.

The data confidentiality solution will identify what data is stored within the laptop and what data protection measures reside within the laptop.

Scenario 6: Privilege Misuse

An employee, leveraging administrator credentials, exfiltrates data for personal gain. The employee prints several sensitive documents and copies the remaining data onto a Universal

Serial Bus. For the purpose of this scenario, the administrator credentials will be considered stolen in a manner that is outside the scope of this project's security architecture.

The data confidentiality solution will provide user access controls to mitigate the ability of users to abuse administrator credentials. The solution will also baseline typical administrator account usage to better understand what behavior is authorized. The solution may also protect against unauthorized printing and use of removable media.

Scenario 7: Eavesdropping

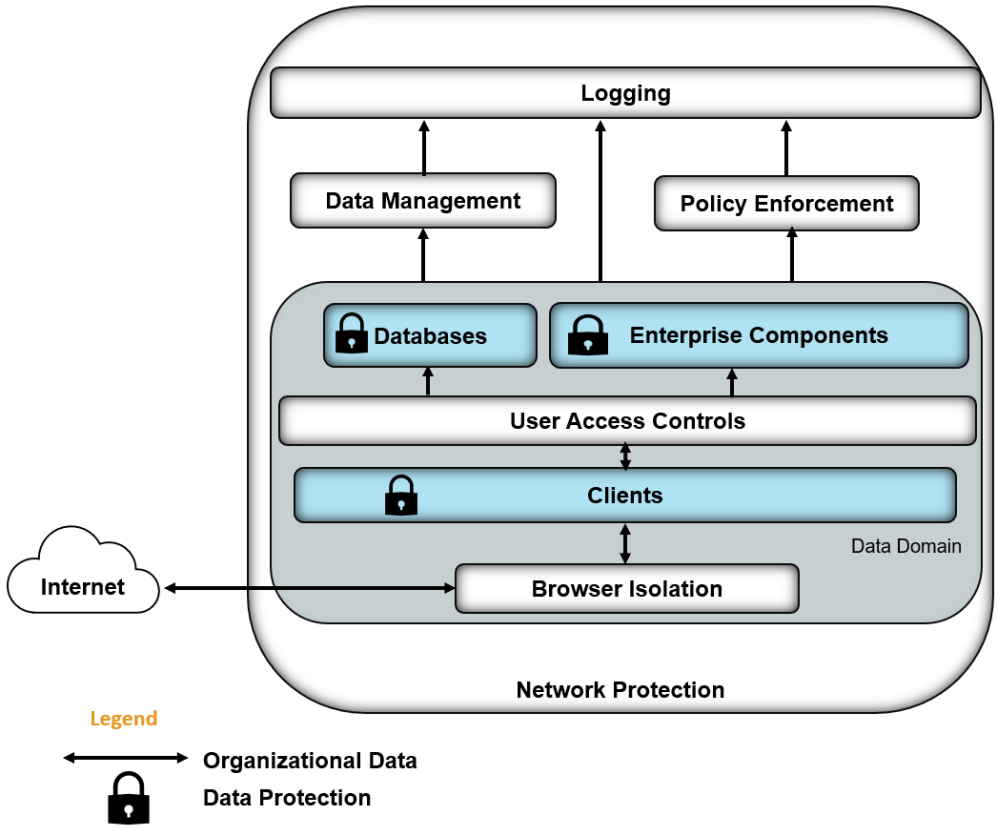
An external actor compromises an organization's network and can hijack network communications via a man-in-the-middle attack, resulting in data loss.

The data confidentiality solution will provide network-level protection against the man-in-the-middle attack.

3 High-Level Architecture

Figure 1 below depicts the integration of capabilities to provide the Functions of Identify and Protect for data confidentiality.

Figure 1. High-level architecture for Identify and Protect functions



Component List

Some components in the architecture, such as databases, are not a part of the components required of the data confidentiality solution to identify and protect. As such, NCCoE will provide

these components with its internal build. The components that are required of the data confidentiality solution include but are not limited to:

- log collection, collation, and correlation
- network protection solution
    - network mapping
    - network segmentation
    - network protection
    - browser isolation
- user access controls
- data management
    - data discovery
    - data inventory
- data protection
    - protection at rest
        - including file- and system-level encryption
    - protection in transit
    - protection in use
- protection against the use of removable media
- policy enforcement

Solution Characteristics

To address the scenarios in Section 2, this project will use a selection of commercially available technologies. The solution will demonstrate the Categories of Identify and Protect of the Cybersecurity Framework [3]. The solution will:

- Identify and inventory data and data flows
- Protect against confidentiality attacks on hosts
- Protect against confidentiality attacks that occur on the network
- Protect against confidentiality attacks that occur on enterprise components
- Protect enterprise data at rest, in transit, and in use
- Protect the network and remote access capabilities
- Provide logging and audit capabilities
- Provide user access controls to data
- Provide user authentication mechanisms

4 Relevant Standards and Guidance

- NIST Federal Information Processing Standards (FIPS) 140-2—Security Requirements for Cryptographic Modules http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- NIST Special Publication (SP) 800-34 Revision 1—*Contingency Planning Guide for Federal Information Systems* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

- NIST SP 800-37 Revision 2—*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- NIST SP 800-53 Revision 4—*Security and Privacy Controls for Federal Information Systems and Organizations*
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST SP 800-57 Part 1 Revision 4—*Recommendation for Key Management: Part 1: General*
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
- NIST SP 800-61 Revision 2—*Computer Security Incident Handling Guide*
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- NIST SP 800-83 Revision 1—*Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf
- NIST SP 800-92—*Guide to Computer Security Log Management*
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
- NIST SP 800-100—*Information Security Handbook: A Guide for Managers*
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf
- NIST SP 800-122—*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
  https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf
- NIST SP 800-150—*Guide to Cyber Threat Information Sharing*
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
- NIST SP 800-175B—*Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175b.pdf
- NIST SP 800-181—*National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*
  https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf
- NIST SP 800-184—*Guide for Cybersecurity Event Recovery*
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

APPENDIX A REFERENCES

[1] "2018 Cost of Data Breach Study: Impact of Business Continuity Management," Ponemon Institute, Oct. 2018.

[2] Tim McBride et al., *DRAFT Data Integrity: Recovering from Ransomware and Other Destructive Events,* National Institute of Standards and Technology (NIST) Special Publication 1800-11, Gaithersburg, Md., Sept. 2017. Available: https://nccoe.nist.gov/publication/1800-11/.

[3] *Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1,* NIST, Gaithersburg, Md., Jan. 2017. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11.

APPENDIX B ACRONYMS AND ABBREVIATIONS

CNSSI	Committee on National Security Systems Instruction
DI	Data Integrity
FIPS	Federal Information Processing Standard
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
SP	Special Publication

APPENDIX C GLOSSARY

Access Control	The process of granting or denying specific requests to 1) obtain and use information and related information processing services, and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances) SOURCES: Federal Information Processing Standards (FIPS) 201; Committee on National Security Systems Instruction (CNSSI)-4009
Analysis	The examination of acquired data for its significance and probative value to the case SOURCE: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-72
Asset	A major application, general support system, high-impact program, physical plant, mission-critical system, personnel member, piece of equipment, or logically related group of systems PARAPHRASED FROM CNSSI-4009
Attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself SOURCE: CNSSI-4009
Audit Log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period SOURCE: CNSSI-4009
Cybersecurity	The ability to protect or defend cyber space from cyber attacks PARAPHRASED FROM CNSSI-4009
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted SOURCE: CNSSI-4009
Data Integrity	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner SOURCE: CNSSI-4009
Data Loss	The alteration or deletion of proprietary, sensitive, personal, or otherwise critical data Note: The definition in NIST Interagency or Internal Report 7298 describes data loss as a loss of confidentiality; for example, when data is stolen and leaked. Here, we refer to data loss as data being destroyed in some way.
Encryption	Conversion of plaintext to ciphertext through a cryptographic algorithm

	PARAPHRASED FROM FIPS 185
Enterprise	An organization with a defined mission/goal and a defined boundary. It uses information systems to execute that mission and is responsible for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, information systems, and information and mission management.
	PARAPHRASED FROM CNSSI-4009
Exfiltration	The unauthorized transfer of information from an information system
	SOURCE: CNNSI 4009-2015
Impact	The magnitude of harm that can be expected to result from unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability
	PARAPHRASED FROM NIST SP 800-60
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
	SOURCE: NIST SP 800-61
Personally Identifiable Information	Any information about an individual that can be used to distinguish or trace an individual's identity, and any other information that is linked or linkable to an individual
	PARAPHRASED FROM NIST SP 800-163
Phishing	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means
	SOURCE: NIST SP 800-83
Ransomware	A type of malware that encrypts data on a system, usually with the goal of selling the data back to the owner for money
	SOURCE: https://www.us-cert.gov/Ransomware
Security	A condition that results from establishing and maintaining protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach
	SOURCE: CNSSI-4009
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access,

	destruction, disclosure, modification of information, and denial of service PARAPHRASED FROM NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; CNSSI-4009
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source SOURCES: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-60; NIST SP 800-115; FIPS 200