PROJECT DESCRIPTION

DATA CONFIDENTIALITY

Detect, Respond to, and Recover from 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

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 detect, respond to, and recover from incidents that affect data confidentiality. The architecture described seeks to provide the technical capabilities needed by an organization to maintain full awareness of its data as well as mitigate the effects of a data breach. The implementation will include data and network monitoring, event detection, and other potential technologies. 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 an organization in detecting, responding to, and recovering from a loss of data confidentiality. Data confidentiality refers to 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 addresses a technical challenge. An example implementation 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 the following questions related to detecting, responding to, and recovering from data confidentiality events:

- What is the baseline activity of systems, networks, and users?
- When has a data confidentiality event occurred, and what was the impact?
- How will an established response plan be executed?
- How can an organization determine what data confidentiality incidents merit response and recovery?
- How will events be contained and mitigated?
- What type of recovery plan should be designed and executed?

This project will address:

- a network baselining solution to establish normal parameters for activity
- an event detection solution with components that monitor:
  - systems, for confidentiality events
  - networks, for unusual activity and potential cybersecurity events
  - users, for all activities, including unusual or unauthorized activity
  - data, for attempted unauthorized access or movement
- an event data aggregation and correlation solution to assist in detecting and responding to a data confidentiality event
- a file access monitoring solution to produce logs and alerts
- an exfiltration detection and mitigation solution to prevent data confidentiality loss
- tools that aid in identification of information that is necessary for a data confidentiality recovery event

This project will not address data security issues related to integrity or availability. This includes violations of machine integrity that can lead to 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.

Assumptions/Challenges

Security Team

The size, budget, and expertise of members of a security team vary significantly among organizations. Both detecting and, to a larger degree, responding to a data confidentiality event depend on qualified security employees to analyze and act on the data presented by cybersecurity tools. This project will make assumptions about the core competencies of an organization’s security team.

Breach Response

An organization's data breach response team will ideally contain nontechnical members who focus on legal, administrative, and public relations, among other necessary issues. While essential for proper breach response, these capabilities will not be covered in the project. This project will assume that the organization can understand and execute its nontechnical responsibilities in the aftermath of a data breach.

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, The NCCoE 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://www.nccoe.nist.gov.

Recovery Capabilities

Given that data breaches can cause disclosure of data to unauthorized parties, removing the data from those unauthorized entities and restoring the original restrictions are nearly impossible, especially if the loss of confidentiality was executed maliciously. Thus, recovery from a data confidentiality attack is not a technological implementation issue; it is a policy-based response. This project will attempt to provide guidance on what artifacts from the event are relevant to the recovery response.

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 DI. They were categorized as data confidentiality challenges.

During the Data Integrity Project, 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 Identifying and Protecting Assets and Data 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 provide monitoring capabilities to help recognize the active breach. The solution will also notify the security team of the activity and respond in accordance with policy that stops the continued data leak (e.g., prevents access to the data).

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 provide monitoring for the security team to recognize that data has been accessed and/or exfiltrated. The solution will also respond with actions that immediately terminate access for the malicious actor to the database.

Scenario 3: Ransomware

An employee is a victim of ransomware and is presented with a note showing contents of 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 provide monitoring and logging to determine the scope and severity of a data breach. The results from the monitoring solution will inform the appropriate response to discontinue the data leak.

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 detect that access is being issued to an individual not authorized and will produce an alert of the error.

Scenario 5: Lost Laptop

A user loses their laptop that contains proprietary company information.

The data confidentiality solution will determine what information was in the laptop and potentially try to remote-delete data.

Scenario 6: Privilege Misuse

An employee, leveraging administrator credentials, accesses data to exfiltrate that data for personal gain. The employee prints several sensitive documents and then exfiltrates the remaining data via Universal Serial Bus. For the purpose of this project, the administrator credentials will have been considered stolen in a manner that is outside the scope of the security architecture.

The data confidentiality solution will provide monitoring to allow the security team to recognize that data has been exfiltrated via unallowable media type. The solution will also respond with appropriate actions to immediately stop the account from having continued access. The time and process of restoring the account will be determined by policy.

Scenario 7: Eavesdropping

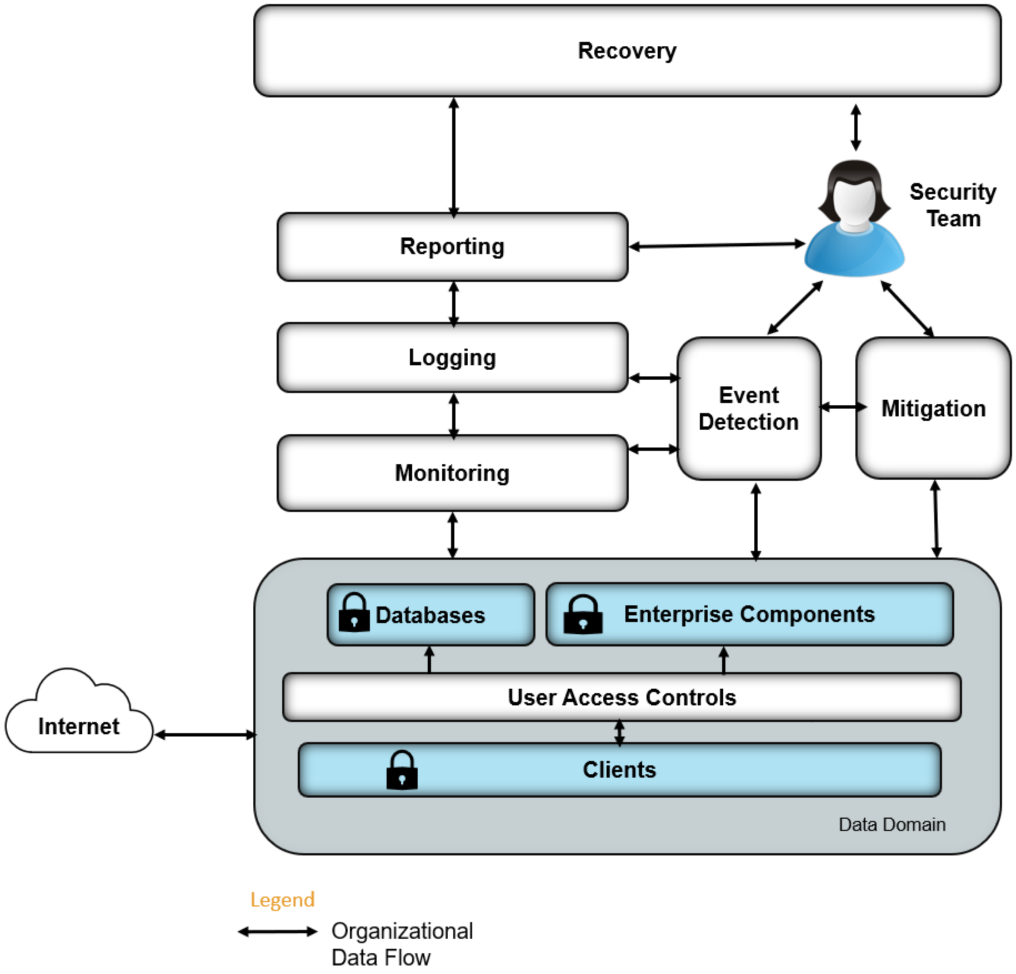
An external actor compromises an organization's network and can hijack network communications via a man-in-the-middle attack, resulting in data loss.

The data confidentiality solution will detect unauthorized network access and respond appropriately to sever the connection.

3 High-Level Architecture

Figure 1 below depicts the proposed high-level architecture that integrates suggested capabilities to address the Functions of Detect, Respond, and Recover.

Figure 1. High-level architecture for Detect, Respond, and Recover 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 detect, respond to and recover from. As such, NCCoE will provide these components with its internal build. The components that are required of the data confidentiality solutions for this project include but are not limited to:

- monitoring
  - file
  - network
  - users
- event detection
  - exfiltration activity
  - unauthorized activity
  - anomalous activity
- log collection, collation, and correlation of all activities within the enterprise

- reporting capability
- capability to mitigate data loss

Solution Characteristics

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

- Monitor the enterprise's user and data activity.
- Detect unauthorized data flows, user behavior, and data access.
- Report unauthorized activity with respect to users and data in transit, at rest, or in use to centralized monitoring and reporting software.
- Analyze the impact of unauthorized behavior and malicious behavior on the network or end points. Determine if a loss of data confidentiality is occurring or has occurred.
- Mitigate the impact of such losses of data confidentiality by facilitating an effective response to a data breach scenario.
- Contain the effects of a data breach so that more data is not exposed.
- Facilitate the recovery effort from data breaches by providing detailed information as to the scope and severity of the breach.

4 Relevant Standards and Guidance

- Office of Management and Budget Circular Number A-130—Managing Information as a Strategic Resource https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
- 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) 800-37 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 800-100—*Information Security Handbook: A Guide for Managers* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf
- NIST SP 800-150—*Guide to Cyber Threat Information Sharing* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
- NIST SP 800-160 Volume 2—*Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems* https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final

- 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
- NIST *Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1* https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

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 Standards
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
SP	Special Publication

APPENDIX C GLOSSARY

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 Committee on National Security Systems Instruction (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

Baselining

Monitoring resources to determine typical utilization patterns so that significant deviations can be detected

SOURCE: NIST SP 800-61

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 Federal Information Processing Standards 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

Incident

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

SOURCE: NIST SP 800-61

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

Malware

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim

SOURCE: NIST SP 800-83

Phishing

Tricking individuals into disclosing sensitive personal information through deceptive computer-based means

SOURCE: NIST SP 800-83

Ransomware

A type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid

SOURCE: https://www.us-cert.gov/Ransomware

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/or 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