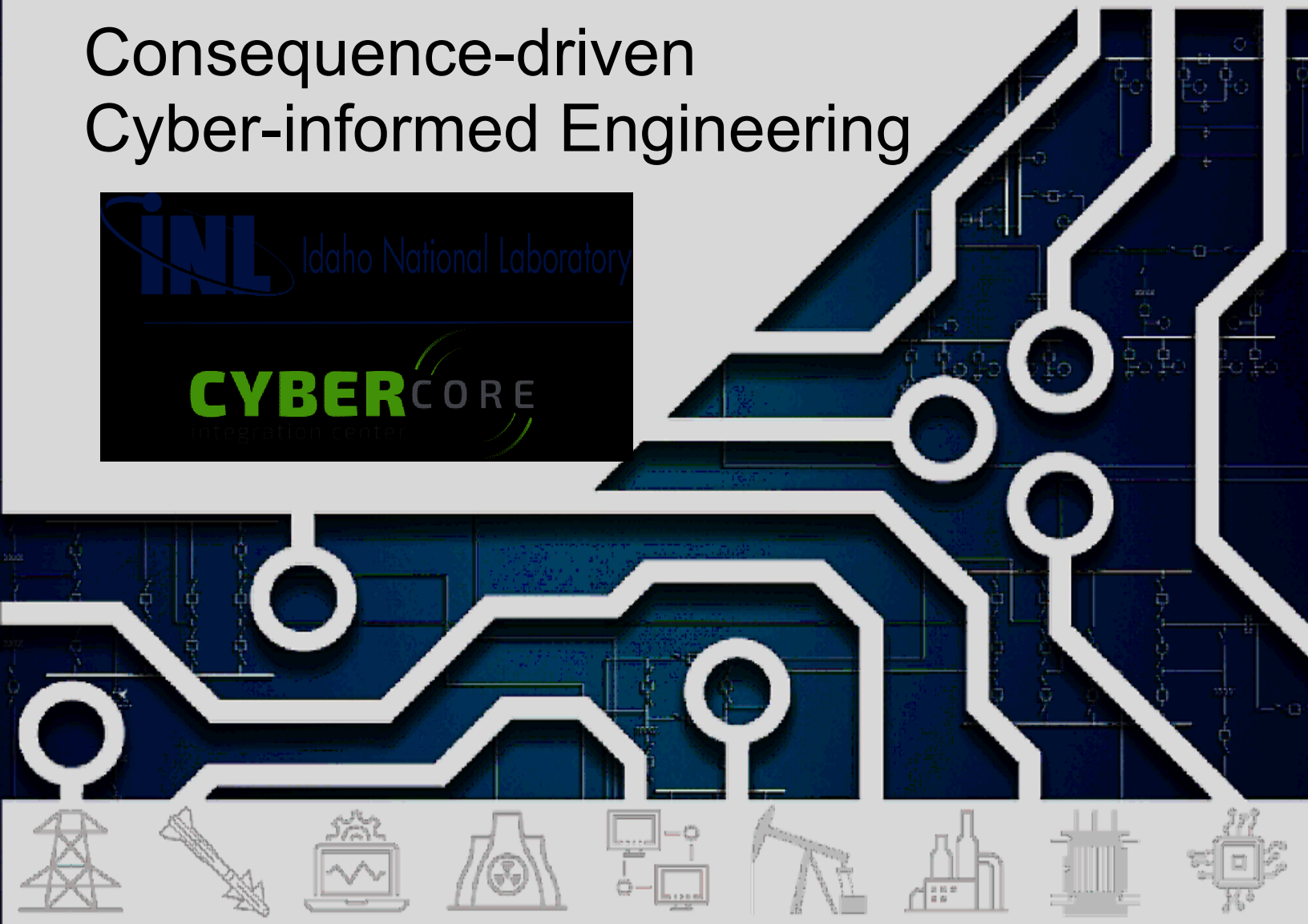
CCE Phase 2: System-of-Systems Analysis

Consequence-driven Cyber-informed Engineering



Prepared By: Doug Buddenbohm and Sarah G. Freeman
Cybercore Integration Center
Idaho National Laboratory

May 5, 2020

INL-EXT-20-58093

CCE Phase 2: System-of-Systems Analysis

Consequence-driven Cyber-informed Engineering

Doug Buddenbohm
Lead Author

Sarah G. Freeman
Co-Author

Idaho National Laboratory
Cybercore Integration Center
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of National & Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

CCE Phase 2: System-of-Systems Analysis

Introduction

During Phase 1, Consequence Prioritization, the CCE Team identified High Consequence Events (HCEs) that can be accomplished through cyber means to impact critical functions, services, and processes. During Phase 2, System-of-Systems Analysis (SoS Analysis), the CCE Team will conduct a systematic review and analysis of information related to the equipment, systems, processes, operations, maintenance, testing, and procurement practices based on the HCEs identified in Phase 1.

The data collected in Phase 2 will serve as the initial input for Phase 3. The SoS Analysis efforts will culminate with the System Description output, designed to summarize the information collected. The System Description functionally describes all aspects of the HCE; as such, it is exceptionally important to consider how the CCE Team will protect this data—*before* it is collected.

During Phase 2, the CCE Team focuses on collecting, organizing, reviewing, and summarizing the necessary information to fully understand the system(s) affected by the potential HCE identified in Phase 1. It is important to consider how various technologies are used within the system, what and where necessary information exchanges occur. For example, the generation site of a utility produces data that must be shared with the Energy Management System (EMS), as well as the Independent Service Operator (ISO), for balancing load. However, the specific design of that information exchange, and even the shared data, may vary from utility to utility.

At times, the operation of an organization may rely on traditional information technology (IT), as well as subcontractors, vendors, and suppliers that reside outside of the organization. SoS Analysis should be inclusive, considering all the entities, architectures, networks, and technologies relevant to an organization's critical functions or roles, regardless of location. The System Description for each HCE is the input for Phase 3, Consequence-based Targeting. A high-level overview of this phase can be found in the Phase 2 process chart on the next page (see Figure 1).

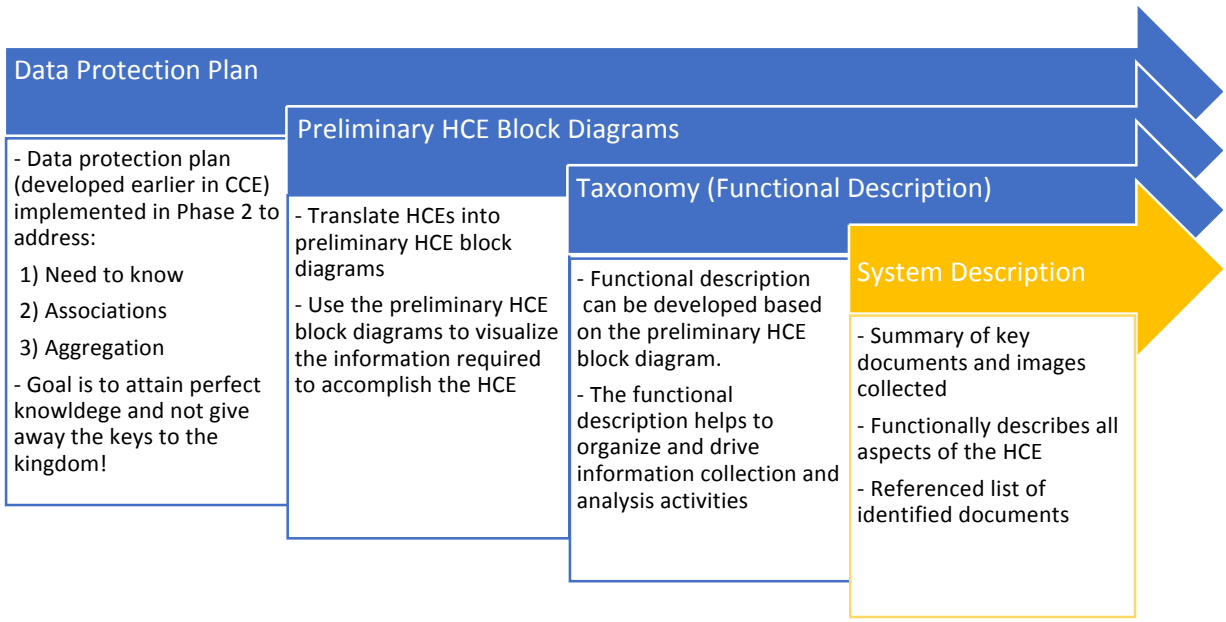


Figure 1. CCE Phase 2 process chart.

Data Protection Plan

Phase 2 collects key information that an adversary could use as a roadmap to target a system and its most important business functions. It is crucial to put in place a data protection plan to protect an organization's data. Don't give away the keys to the kingdom! The aggregation of data and documentation in Phase 2 can give the adversary full inside knowledge/access to key systems. Initially, adversaries do not fully understand the targets they have chosen—even if they have a general idea, there are still large knowledge gaps. Only an organization knows in detail how a process works, who is involved in each function, what third parties are involved, and how equipment and systems are implemented. This insider's advantage is known as **perfect knowledge**. If perfect knowledge data is not properly protected, it gives the adversary an advantage and possibly the knowledge required to successfully target key systems.

Ensure that a data protection plan is developed, properly implemented, and practiced. Equally as important, be sure the entire CCE Team understands their responsibility in keeping this information secure (i.e., not sharing or forwarding any documents, working on sensitive items on unauthorized computers/networks, or discussing the system of systems with individuals that lack a valid business reason).

Data Classification Criteria

Data should be categorized and protected according to sensitivity. Access should be limited and based on a "need to know." Information derived from the data should also be protected and categorized, based on the potential risk of damage that could occur from unauthorized disclosure. See Figure 2 on the next page for a brief description of the three criteria that factor into data classification.

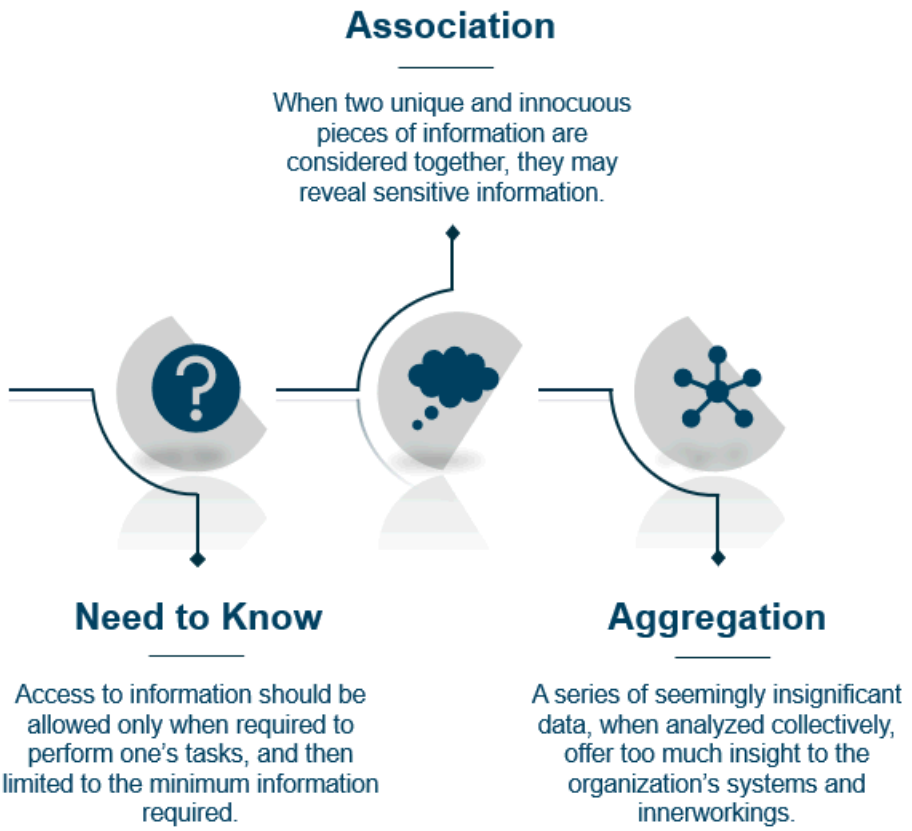


Figure 2. Data classification criteria.

Consider the following criteria that factor into data classification:

a. **Need to Know**: This is the fundamental security principle in safeguarding information. Requiring a need to know for data access ensures that such information is available only to those persons with appropriate managerial approval who have met clearly identified requirements. For example, a third-party vendor and the CISO should have different levels of access because they require different levels of need to know to accomplish their tasks.

b. **Aggregation**: Individually insignificant or apparently unimportant items or information that, when combined, reveal system details, objectives, requirements, plans, or other sensitive aspects of an organization's business mission. The disclosure of such information would provide insight into sensitive or mission critical activities, capabilities, vulnerabilities, or methods. Information amassed or collected in one location should be protected.

c. **Association**: The significance of information often depends upon its context. Therefore, when two unique and innocuous pieces of information are considered together, they may reveal sensitive information. For example, consider two unique facts: Siemens manufactures controllers, and a company publishes a job announcement for someone with Siemens controller experience. An adversary may be able to use this announcement to accurately draw a conclusion about the sensitive fact that the company uses Siemens controllers.

It is important that organizations recognize that creating this aggregated data may be dangerous for their organization, but not collecting these data (and ignoring the associated risks that already exist) is more dangerous.

Consider the following types of information to protect:

- Information in a storage medium that has been removed from another information system, or information that has been inadvertently stored in or transferred through an unprotected system.
- Information describing the nature, exploitation, or location of a system vulnerability, as well as the descriptions of the procedures required to remove/mitigate the vulnerability. In situations where mitigations only partially limit exploitation, the vulnerability information is still sensitive and must be protected.
- Information that could reveal, jeopardize, or compromise a device, piece of equipment, or the technology used in a system.
- Information pertaining to a system that reveals capabilities or weakness that would provide insight or motivate an adversary to develop malware or an exploit.
- Description of the design, capabilities, and functions of an information system[1] (or software developed to process that information) could reveal a method or reduce the level of effort for an adversary to achieve an objective.
- Information that reveals organizational structure, job posting specifics, and staffing levels may provide insight to an adversary.

Preliminary HCE Block Diagrams

After revisiting and developing the data protection plan for Phase 2, the CCE Team creates a simple, high-level diagram for each HCE. These preliminary HCE block diagrams help visualize the information required to accomplish the outcome. This exercise helps narrow the scope of analysis, organize the physical and functional connections between the target components and the affected systems, and minimize the volume of information collected to describe each HCE. The preliminary HCE block diagram provides a starting point for identifying what information and system accesses the adversary needs to accomplish the HCE. This information steers the data collection efforts.

Taxonomy (Functional Description)

Most of the activity in Phase 2 will involve identifying, collecting, and organizing documentation relevant to an HCE. This information is used to build a comprehensive knowledge base of key details for the SoS Analysis. The goal is to obtain perfect knowledge of the system(s) relevant to the HCE. To help organize the collection and analysis activities, a taxonomy or functional description can be developed based on the preliminary HCE block diagram. This is often best done by starting with the target components that must be affected to cause the HCE and working backwards. Considering the following:

- What systems and equipment are involved in the HCE?
- What documentation is needed to describe interconnected systems and dependencies?
- What relationships with other entities are involved?

[1] Information system refers to any telecommunications and/or computer-related equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange transmission, or reception of voice and/or data (digital or analog), including software, firmware, and hardware.

The functional description can be represented as a hierarchical data structure or taxonomy. Using this functional description as the basis for investigation, the CCE Team will begin collecting and organizing key details. Relevant information to support this work includes details of interconnected systems and dependencies, controllers, technical manuals, diagrams, protocols, access lists, associated manufacturers, trusted relationships, contractors, suppliers, emergency procedures, and personnel. The SoS Analysis proceeds in parallel during information collection by building an understanding of the critical systems and processes.

Recall both the data collection effort and the CCE methodology are iterative. As the CCE Team identifies specific information gaps from the SoS Analysis, time is taken to adjust the detailed information collection to close these gaps. While not all-inclusive, the resulting information will build upon the preliminary HCE block diagram. This will ideally result in a body of perfect knowledge. This will benefit the organization by both identifying critical information and determining where it resides.

For example, is the critical information on internal servers or a public-facing server? To help ensure continued data collection efforts remain focused on the HCE, it may help to build out the original diagram throughout Phase 2. This helps produce diagrams with greater detail as more data is collected and aggregated. The point of Phase 2 is to be aware of all the information that an adversary would need to execute a successful attack.

System Description

In order to analyze the system to develop a targeting plan, the CCE Team must collect as much relevant information as possible and then summarize the key details to support a deeper level of knowledge of the system operations, personnel support activities, system configuration, and other aspects of the operation. To accomplish this, a **System Description** is developed that details the key information that an adversary may need to obtain access and accomplish the HCE through cyber means. This description should detail all the elements in the preliminary HCE block diagram and provide traceability to all the information collected in Phase 2, including where it resides and who has access to it. This System Description will be the output of Phase 2 and the input to Phase 3.

See Idaho National Laboratory's document titled "CCE Case Study: Ukraine Substation Power Outage" (INL-EXT-20-58092) for more Phase 2 examples on creating preliminary HCE block diagrams, taxonomies, and System Descriptions.