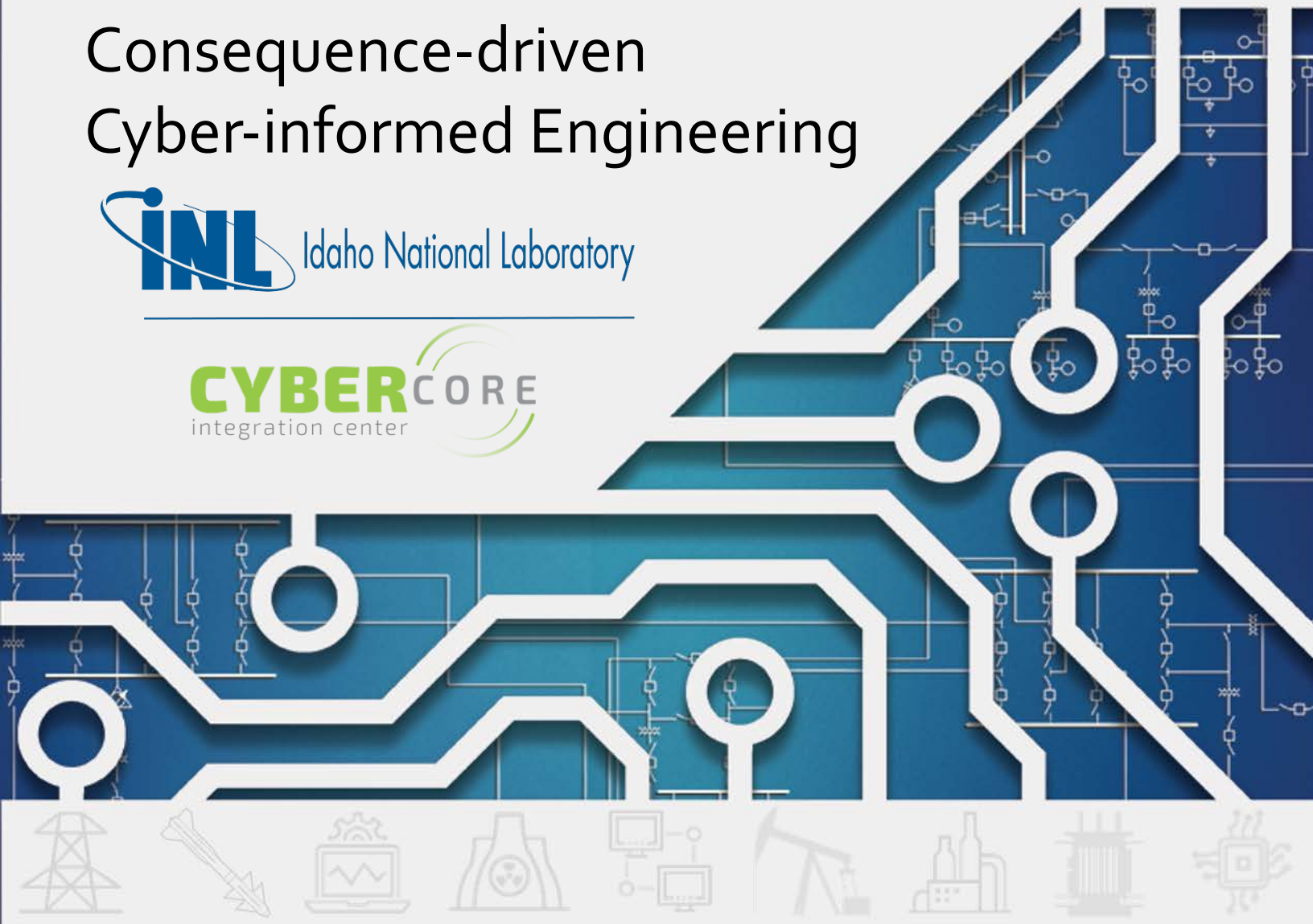
# CCE Phase 4: Mitigations and Protections

## Consequence-driven Cyber-informed Engineering



Prepared By: Theodore Miller and Sarah G. Freeman
Cybercore Integration Center
Idaho National Laboratory

May 5, 2020

INL-EXT-20-58091

# CCE Phase 4: Mitigations and Protections

## Consequence-driven Cyber-informed Engineering

**Theodore Miller**
**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 4: Mitigations and Protections

## Introduction

During the first three phases, the CCE Team identified any instances of unverified trust in the organization's technologies, processes, and procedures, any or all of which could be used to adversely impact the system. In Phase 4, the primary goal is to remove the possibility of the end effect—that is, to develop means or mechanisms that will ensure an adversary cannot achieve their Objective (identified in Phase 1) via cyber means. Such measures are known as "protections."

In some cases, this may not be possible, or the implementation of protections may not be desirable due to other considerations. In such cases, means and mechanisms should be developed that focus on putting an organization in a better position to identify adversary activities directed against it, increasing the cost of cyber-enabled sabotage for the adversary (including making things more difficult for the adversary and attempting to lower the chances an adversary may succeed), or decreasing the recovery cost of a victim organization. These measures are known as "mitigations."

## Categorizing CCE Mitigations and Protections

In CCE, mitigations and protections are categorized by their function. Some options are designed to completely stop an attack, whereas others are implemented to thwart or discourage an adversary from being successful. The mitigation and protection functions in CCE were inspired by NIST's Five Functions.[1] CCE employs the NIST framework as a guideline for categorizing mitigations and protection options identified during Phase 4. As of April 2020, NIST's website[a] listed NIST's five functions as:

1. **Identify:** Assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities.
2. **Protect:** Outlines appropriate safeguards to ensure delivery of critical infrastructure services.
3. **Detect:** Defines the appropriate activities to identify the occurrence of a cybersecurity event; enables timely discovery of cybersecurity events.
4. **Respond:** Supports the ability to contain the impact of a potential cybersecurity incident.
5. **Recover:** Identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident; supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

The focus of Phase 4 in CCE is on the last four of NIST's Five Functions: Protect, Detect, Respond, and Recover. The Identify function is covered in previous phases, particularly during Phase 2.

[1] The NIST Five Functions were developed in response to the February 2013 passage of Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity." As part of this order, National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework, based on existing standards, guidelines, and practices, for reducing cyber risks to critical infrastructure. The Department of Homeland Security has used this framework to assist critical infrastructure organizations in aligning their security goals with available resources. Additional information can be found at https://www.nist.gov/cyberframework/online-learning/five-functions.

To better address CCE's goal of protecting critical infrastructure, CCE uses its own definitions for these four functions; however, the principle behind each remains largely the same:

1. **Protect:** The ability to remove the objective of cyber-enabled sabotage (take it "off the table" for an adversary)
2. **Detect:** Enables timely discovery of adversary activities.
3. **Respond:** The ability to contain or disrupt adversary activities.
4. **Recover:** Timely restoration of critical functions and services.

Protections address the "Protect" function, while mitigations address the "Detect," "Respond," and "Recover" functions. These three do complement each other, and some mitigations may address elements of all three.

## Protect

CCE places heavy emphasis on the "Protect" function, as such actions will—if implemented properly—effectively make it impossible for the adversary to cause a given HCE via cyber means.

As an extremely simple example, consider a liquid storage tank at an industrial facility. A PLC governs the pump controlling the fill level of the tank. If an overfill of this tank represents an HCE, a possible protection mechanism is the use of a separate float switch in the tank that, upon activation, will physically disconnect the pump from the power supply. By installing such a device, an adversary will not be able to cause this HCE by cyber means alone.

## Detect

The "Detect" function focuses on creating a means to quickly identify adversary activity. In effect, this means identifying any attempt at cyber-enabled sabotage in progress—before the adversary can achieve their objective. It is important to note that the Detect function includes all types of adversary activities—not just network activity. This could also include a shipment of a critical components not arriving, a cyber-attack at a vendor or supplier, or unexplained behavior of critical systems.

If an organization can quickly identify adversary activity, that organization has a better chance at minimizing damages. The December 2015 Ukraine power outages provide an example of this. In at least one instance, months in advance of the actual outage, a Ukrainian power company detected an adversary in the corporate network and took corrective action. Although they were not successful in taking away adversary access to their network, the hassle this presented to the adversary may have spared the organization from an attack in the end. None of the victim companies detected any adversary activity in advance of the outage.

## Respond

The "Respond" function seeks to equip the appropriate individuals with a plan regarding what to do if an Event is in progress. The response plan should help to contain, disrupt, or otherwise prevent further adversary activity.

## Recover

The "Recover" function aims for the complete restoration of normal operations, including whatever actions are needed for that to occur. This may differ from returning to operation, particularly if it is possible to operate in a degraded state.

## Development of Mitigations and Protections

To begin developing ideas for protection and mitigation, it may be useful to conduct a structured brainstorming session. Participants for these sessions should include both the CCE Team and individuals who have not participated in previous CCE work. Ideally, participation will include SMEs *not* previously involved in the process, as such individuals may be able to examine the situation with a greater degree of objectivity.

Consider the potential advantages of having all participants in the same room at once. If this is not possible, multiple rounds of individual input may be required. Alternatively, a Delphi Method or similar design may be implemented to enable elicitation of SME expertise remotely.

The meeting should begin with an overview of what CCE is, the CCE Team's progress, key findings, and opportunities for improvement. Once everyone is on the same page, the team may choose to present all Attack Scenarios developed in Phase 3 to get a sense of the larger picture and detect any commonalities.

Brainstorming mitigations will start with a walkthrough of each Attack Scenario. During the meeting, members of the CCE Team discuss methods of eliminating threats when possible and plan mitigation actions when it is not, or as a secondary option.

As this brainstorming begins, the CCE Team will consider opportunities to strengthen security or simplify processes in a way that reduces or removes risk. To assist this effort, the CCE Team should review each fully developed Attack Scenario from Phase 3 and the associated System Targeting Description for each HCE. As each Attack Scenario is reviewed, the team may need to confirm details to assure suggested mitigation methods will be successful and not problematic for operations.

As methods are brainstormed, it is recommended that the CCE Team diagram appropriate mitigations and protections, so the entire group has a clear and concise understanding of proposed methods. This will also help the team identify patterns from one Attack Scenario to the next, allowing for the recognition of a reliance on a repeated solution and identification of potential improvements.

## Prioritization of Mitigations and Protections

There is no all-purpose method for prioritizing mitigations and protections, although it may prove beneficial to at least consider the following:

- **Type ("Protection" vs. "Mitigation")**: Protections will prevent an adversary from causing an HCE via cyber means. Mitigations cannot do so.
- **Efficacy**: Proposed protections or mitigations should be reviewed for their perceived efficacy—whether the proposed solution makes the attack not feasible, or to what degree it can reduce any negative consequences or make things more costly or challenging for an adversary. This kind of review is limited in that the efficacy of a solution ultimately relies on the specific implementation that is adopted.
- **Existing Threat Information**: Some attack scenarios may leverage techniques that have already been witnessed "in the wild" (deployed against a victim) or involve targeting of systems or components that correspond with known adversary interest. The presence of existing capability or research directed against these systems will presumably result in an increased likelihood that an adversary would first pursue these options over other scenarios.

- **Assessed Attack Difficulty**: An increase in attack difficulty will presumably correspond with a decrease in the likelihood that an adversary would first pursue such a path, due to the increase in relative cost and/or the increased need for specialized skills or knowledge. In such an evaluation, the difficulty ranking can be baselined at the level of the least challenging scenario.

The most promising solutions identified will receive subsequent attention from members of the CCE Team, along with any relevant SMEs, to develop a plan for presentation to the organization's decision makers.

## Implementation of Mitigations and Protections

Limited resources, such as time, money, and available personnel, will affect how quickly a protection or mitigation can be implemented. With limited resources, it is up to each individual organization to decide which protections and/or mitigations to implement, or whether they can be implemented at all.

The point is that the decision makers will ultimately be able to make a fully informed decision. The worst case is for an organization to accept risk it doesn't know about.

The CCE Team will present recommended mitigations to the appropriate decision makers within the organization. As members of the CCE Team may not necessarily "speak the same language" as individuals who work at the C-suite level, it will likely prove beneficial for the CCE Team to consciously frame such a presentation around the concept of risk management as opposed to focusing on the technical details of a given HCE and suggested mitigation strategies. Feedback from the C-suite may be incorporated as required to develop final mitigations for implementation.

Any programmatic and design changes have the potential to introduce additional risk. The eventual pursuit of any of these changes should involve a thorough cost-benefit analysis and review after a specific and detailed implementation plan has been developed. This review will determine any potential unidentified consequences and/or risks that may be introduced with these changes.

Some suggested factors to evaluate prior to the implementation of any changes are the burden and cost of implementation and maintenance—again, the emphasis on these considerations is dependent on the organization in question.

See Idaho National Laboratory's document titled "CCE Case Study: Ukraine Substation Power Outage" (INL-EXT-20-58092) for more Phase 4 examples on developing and implementing mitigations and protections.

## Outcomes

The goal of Phase 4 is to develop strategies to eliminate the possibility of an adversary achieving their objective via cyber means, or to develop strategies to detect, respond to, and/or recover from adversary activity.

CCE is intended to serve as a triage activity. In some cases, it may not be possible to prevent an adversary from achieving their objective. In such cases, defensive actions should focus on increasing the resources required of an adversary to perform cyber-attacks or decreasing the resources a victim organization will need for recovery purposes.

The CCE Team is to develop these strategies. Ideally, they will identify several options. The CCE Team will then present these strategies to the organization's senior leadership team, who will ultimately make decisions regarding implementation, and how to best use the organization's resources to manage the identified risk.

[a] National Institute of Standards and Technology (NIST). U.S. Department of Commerce. "Cybersecurity Framework: The Five Functions." Created April 12, 2018, Updated August 10, 2018. Accessed April 3, 2020. https://www.nist.gov/cyberframework/online-learning/five-functions.