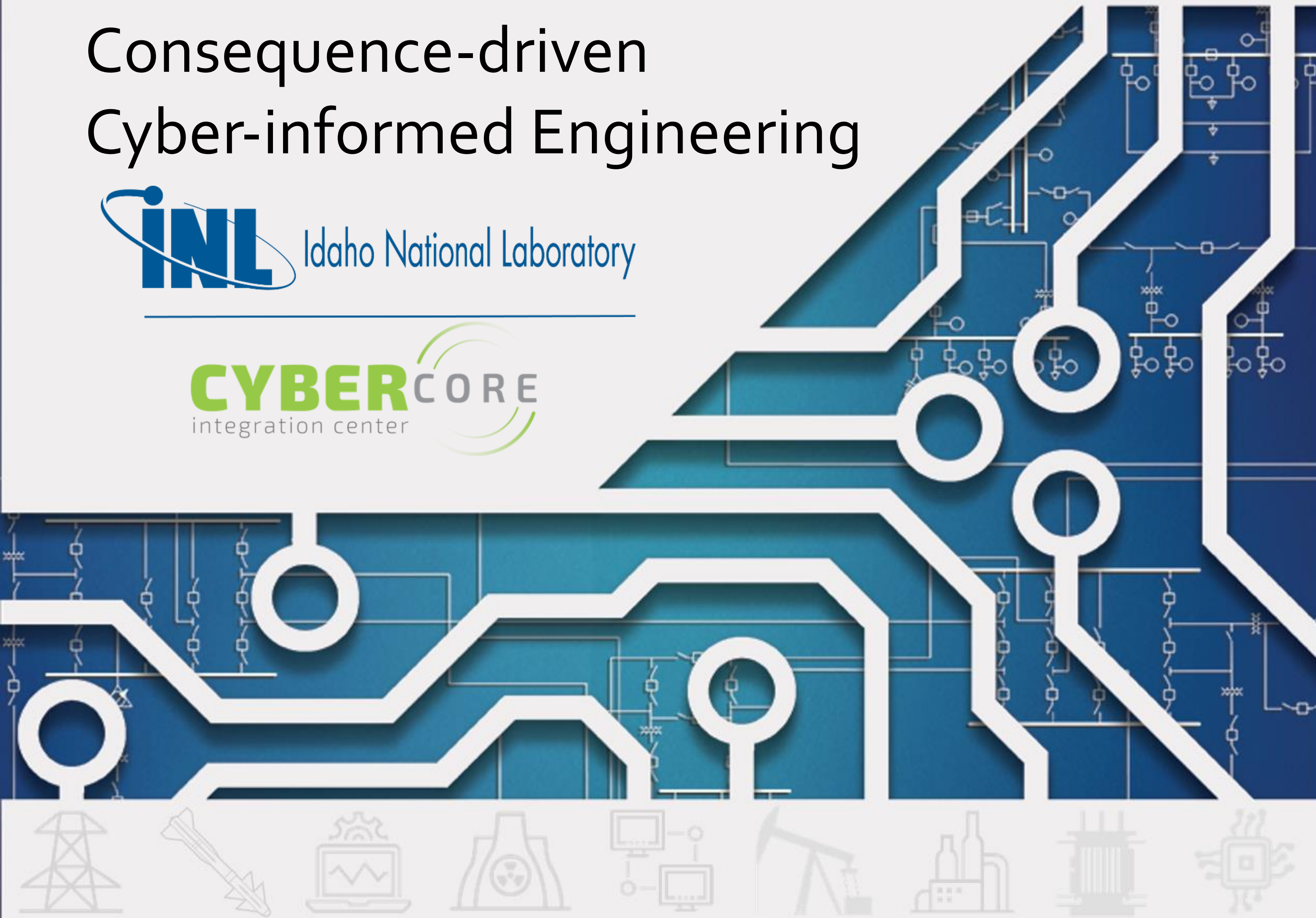
CCE Phase 1: Consequence Prioritization

Consequence-driven Cyber-informed Engineering



Prepared By: Sarah G. Freeman, Nathan Hill Johnson, and Curtis P. St. Michel
Cybercore Integration Center
Idaho National Laboratory

May 5, 2020

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL-EXT-20-58089

CCE Phase 1: Consequence Prioritization

Consequence-driven Cyber-informed Engineering

Sarah G. Freeman
Control Systems Cybersecurity Analyst

Nathan Hill Johnson
Control Systems Cybersecurity Analyst

Curtis P. St. Michel
Cybercore Technical Director

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 1: Consequence Prioritization

Introduction

Idaho National Laboratory (INL) developed the Consequence-driven Cyber-informed Engineering (CCE) methodology to provide public and private organizations with steps to work collaboratively and establish a working relationship to protect critical infrastructure and other national assets. This process is a considerable undertaking, iterative in nature, and—as time and resources allow—should become a part of a company's culture. By focusing on the impact of potentially negative Events, CCE provides a better understanding of how and why adversaries can affect critical functions and services using cyber-enabled sabotage.

The CCE methodology consists of four phases:

Phase 1: Consequence Prioritization

> During this phase, the CCE Team works together to develop the boundaries and thresholds for Events and cyber-Events that could be catastrophic to the organization. They are then prioritized to determine which can be deemed High Consequence Events (HCEs).

Phase 2: System-of-Systems Analysis

> Here the team maps out the systems and processes related to the HCEs identified in Phase 1, and then investigates the dependencies and "unverified trust" which would enable them.

Phase 3: Consequence-based Targeting

> The team refines and develops the targeting requirements an adversary would need to fully understand the attack in detail and, consequently, carry it out.

Phase 4: Mitigations and Protections

> In the final phase, the priority is to take the possibility of the physical effect through cyber means out of the equation using engineering or process changes. If this is not possible, use the detailed targeting requirements developed during Phase 3 to detect adversary activity and implement other types of mitigations.

Consequence Prioritization

This document describes the process for Consequence Prioritization, the first phase of the CCE methodology. The primary goal of Consequence Prioritization is to identify potential disruptive cyber-Events—that is, physical Events that are achievable through cyber means—that would significantly inhibit an organization's ability to provide the critical services and functions deemed fundamental to their business operations or mission.

These disruptive cyber-Events, defined as High Consequence Events (HCE), could include failures or natural disasters, but they should also include cyber misuse of systems and the unique digital dependencies of critical infrastructure assets. While other efforts have been initiated to identify and mitigate disruptive cyber-incidents at the national level, such as Presidential Policy Directive 41,[a] this process is intended to be used by individual organizations to complement those efforts.

Described another way, Consequence Prioritization considers threats greater than those addressable by standard cyber-hygiene and includes the consideration of events that go beyond a traditional continuity of operations (COOP) perspective.

Finally, Consequence Prioritization is most successful when organizations adopt a multi-disciplinary approach, engaging both cybersecurity and engineering expertise, as in-depth engineering perspectives are required to recognize, characterize, and mitigate HCEs. Figure 1 provides a high-level overview of the prioritization process.

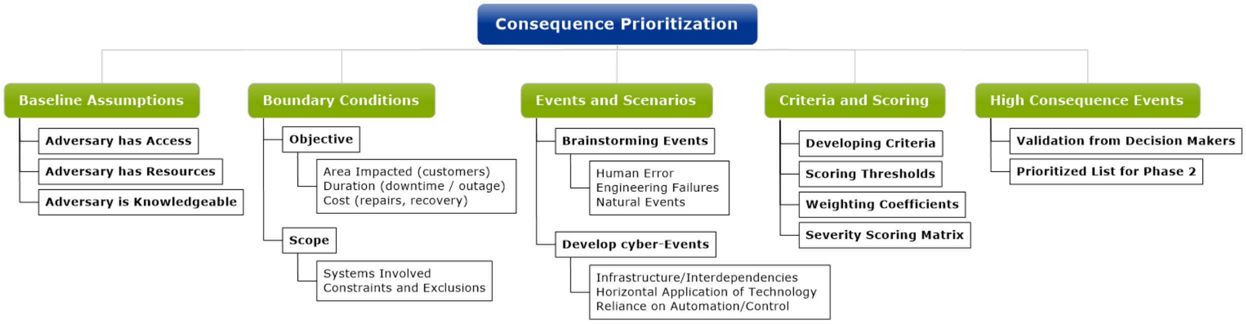


Figure 1: CCE Prioritization method overview.

Establish Baseline Assumptions

Baseline Assumptions:

- **Access has been achieved**
    - Adversary has logical and physical access, including all credentials, IP addresses, firewall and application access, distribution management system (DMS) access, distributed control system (DCS) access, etc.
- **Adversary is knowledgeable**
    - They understand critical equipment and processes and possess the knowledge required to impact the system.
- **Adversary is well-resourced**
    - They have access to the required equipment, engineering expertise, and tools.

[a] President Barack Obama's Presidential Policy Directive 41, "United States Cyber Incident Coordination," July 26, 2016, can be found at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

Objective, Scope, and Boundary Conditions

The CCE Team's first step should be to formally establish and finalize the Objective, Scope, and Boundary Conditions for the CCE engagement. These scoping tasks help better define the area or scale of interest. These concepts must revolve around the critical functions and services that the organization provides. These critical functions and services make up the purpose or mission of the company or organization, and they often have a direct impact on the community or nation. For a large organization which provides services deemed essential to national interests, those interests often become part of the Boundary Conditions.

Rather than focus on some aspects of likelihood of a cyber-attack (such as intent), Consequence Prioritization is primarily concerned with the *impact* of a potential adverse Event. Boundary Conditions should be agreed upon by all party members before generating potential Events.

Objective:

- **Adversarial viewpoint vs. entity viewpoint**
  - Adversaries will determine the degree and type of impact or damage (physical, financial, reputation, etc.) from a cyber-attack when establishing their objectives.
  - The entity (specifically the organization's decision-making group) knows better than anyone what level of impact their organization can withstand before such an attack becomes unbearable.
  - These two viewpoints combined create the Objective in CCE.
- **Examples**
  - **Amount of supply or firm load affected**
    - This is the amount of supply (i.e., generation capacity) loss necessary to be considered significant, which may vary from asset owner to asset owner.
  - **Cost of damage**
    - This is the amount in dollars of damage necessary to impact operations or the mission.
  - **Duration of outage**
    - This is the length of outage time necessary to impact customers and business operations.

Scope:

- **Systems to be examined**
  - Based on ownership and understanding, what relevant systems, processes, and components can be investigated?
- **Constraints or exclusions**
  - An organization may not have control or oversight over certain portions of their operations (e.g., water supply, other basic utilities). These need to be identified and can be excluded from the Scope.

    - Ideally, all entity assets should be made available. In practice, however, some limitations can occur and are most often due to time, financial, or legal constraints (e.g., geographical restrictions or insufficient workforce).

Boundary Conditions:

- **Combination of Objective and Scope**
    - If the Objective is based on a specific monetary threshold of one million dollars, and the Scope includes all the transmission systems of the company, the two are simply combined to form Boundary Conditions.
    - Anything that exists in the Boundary Conditions should be clearly explained in either the Objective or Scope.
- **Example Boundary Conditions**
    - "An outage directly tied to the transmission lines, substations, or connected systems (logical or physical), from which the repair or recovery exceeds the cost of one million dollars."

Events

Next, the CCE Team should generate possible disruptive Events related to the Boundary Conditions. As mentioned previously, a disruptive Event is an end effect that would significantly inhibit an organization's ability to provide the critical services and functions deemed fundamental to their business operations or mission.

As the team works to generate these Events, the ideas should not be limited to traditional or obvious forms of cyber-attacks. It is important to consider similar events that resulted from human error, engineering failures, or natural disasters. In addition, the misuse or destruction of unique digital dependencies for critical infrastructure assets should be considered. This is done to ensure that more creative—or subtle—cyber-enabled sabotage is not overlooked.

Once a full list of Events has been generated, the CCE Team should carefully review the list to screen out any Events that cannot be achieved by cyber means. Those remaining Events are considered cyber-Events that can be partially developed for evaluation.

Developing cyber-Events

Each Event approved by the CCE Team will need to have a high-level explanation added to it. This will describe, in basic terms, how the Event could be achieved via cyber-means. This often includes mention of which systems could be leveraged to accomplish the attack. It is useful to understand the following targeting considerations during this process:

Physical Infrastructure and Interdependencies

The first category of targets to consider is physical infrastructure and interdependency areas. First consider the *physical elements* that are utilized in the performance of a defined process function. Example elements to consider within the electric sector may include generation, substation, transmission and distribution lines, control center facilities, and other components of the power system. Next, identify any interdependencies or chokepoints in the infrastructure. Specific examples include:

Infrastructure Example:

> Impacts to transmission lines near a power generation facility with intent to have multiple electric infrastructure impacts at the power delivery chokepoints. The primary resulting impact of an attack on the transmission system is larger than just an impact on one line because there will be resulting power flow imbalance across the transmission network, as well as disturbances to the underlying distribution system. Additional effects would impact power generation facilities due to the loss of a delivery path for the power produced.

Methods of affecting transmission line infrastructure could include targeting the overcurrent protection of physical assets, and then mis-operating devices to cause physical effects. Transmission substations and switchyards contain a wide variety of electrical infrastructure elements that can be mis-operated to impact the energy flow on the transmission lines. These elements may include breakers, switches, transformers, protection relays, voltage load tap change, capacitor banks, and circuit reclosers.

Interdependency Example:

> For an electric utility with assets that include gas-fired electrical power generation station(s), a “chokepoint” example would be the natural gas delivery system, most typically a pipeline infrastructure. The power generation plants are dependent on the natural gas delivery system and/or natural gas supplier (in the natural gas supply chain, this describes the natural gas producer, which can often be a company separate from the natural gas delivery/pipeline asset owner). The chokepoint could be targeted directly (delivery system or production system attack) or indirectly (attack on the asset owner of the delivery system or production system).

Horizontal Application of Technology

The second category of targets to consider is locations where technology is widely deployed, either within a system or across a geographic region. Additionally, the horizontal application of technology may refer to technology that supports a function performed by multiple organizations. Consider function-specific, widely deployed ICS technologies belonging to the same technology vendor platform, like vendor-specific implementation models of PLC’s, RTU’s, protection relays, meters, etc. Often, single or even multiple instances/versions of these devices may be deployed throughout a critical infrastructure business enterprise for both geographically dispersed and localized asset models.

Another aspect to consider is the increased “depth” of a technology deployment; that is, there is an incentive to develop and adopt vendor solutions that integrate new and previously deployed, legacy technologies through common programming and monitoring applications. This broad and deep functional coverage within the systems is also attractive and valuable to a potential threat actor.

Horizontal Application Example:

> An electric utility may consolidate on a specific RTU vendor to drive consistency from site to site and reduce the level of system complexity for their field personnel. If a payload targeting the common device was deployed throughout a service territory through targeting and misuse of engineering or maintenance software/procedures, the corrective actions to repair/replace the compromised hardware would be extremely time consuming, if not impossible from a workforce perspective.

> From a distribution perspective, consider a smart meter worm that spreads throughout a smart meter infrastructure peer-to-peer mesh network, exploiting the common protocol and common meter firmware, and leverages the built-in capability to disconnect customer power. This creates an opportunity for an adversary to target consistency in architecture, protocols, and devices. This also provides a long deployment lifecycle for valuable exploits.

Reliance on Automation and Control Capabilities

The third category of targets to consider is made up of those which inhibit an organization's automation or control functions. Within most critical infrastructure sectors there is a desire for guaranteed reliability. To achieve highly reliable delivery of services, there needs to be a system that can detect faults or system events and automatically respond or reconfigure to continue to provide services. Within most critical infrastructure organizations, there are systems and processes that have been automated in order to provide functionality that cannot be delivered manually with the necessary real-time response to ensure system reliability and safety.

Consider the various levels of the electric sector. Power generation facilities, regardless of fuel type, rely heavily on resource inputs like automated fuel management systems, feed water systems, water cooling systems, unit control systems, voltage regulation, and a wide variety of system protection controls that prevent damage or mitigate safety risks. An adversary can target any one of these automated systems individually, or he may recognize the redundancies in place and choose to misuse or manipulate multiple systems simultaneously.

Within the electric transmission and distribution systems, there are automated components designed to detect a line fault or another physical condition that may have been caused by a downed power line or pole, and automatically isolate that line through the operation of switches, relays, or breakers. In addition, other elements within the electric system may be switched in around the fault in order to deliver power to as many customers as possible, while responding to the line event. With an understanding of the recovery process, an adversary can send false data to these automated devices to cause mis-operations or reconfigure the devices in a manner so that they will mis-operate under normal conditions. The tendency for electric utilities to use common device types and communications infrastructures can make this an attractive target for an adversary.

Electric Control Center environments contain entire systems that are designed to monitor and act both manually and automatically across a wide footprint of the electric system. This may include hundreds or thousands of substation environments, dozens of power generation facilities, and thousands of miles of transmission lines. The energy management systems (EMS) located at control centers are used to keep the system in balance; however, in the event of certain conditions, a control center operator may have to intercede by increasing generation to service load or shedding load to keep the system in a reliable state. An adversary with an understanding of this capability can target the EMS components to initiate load shed events or manipulate data in a manner that makes an operator believe certain conditions exist that would require operator actions to prevent a wider scale outage.

Automation and Control Examples:

- Natural gas pipeline station volume and/or pressure control, compressor control, and station emergency shutdown sequencing, which includes modern distributed safety systems (flame, gas, etc.)
- Any “real-time” remote monitoring and/or control of assets
- Same day modifications to natural gas receipt and delivery volumes
- Timely collection of accurate volume, gas constituent, and operational parameter data in a geographically dispersed set of system assets
- Electric utility EMS and energy load balancing systems
- Power system area balancing through Automatic Generation Control and scheduling
- Power element maintenance ticketing and electronic-tagging systems
- Use of automatic load shedding schemes within the EMS (Special Protection Schemes [SPS], Remedial Action Schemes [RAS])

Evaluate Potential High Consequence Events

Determine Severity

The Boundary Conditions established previously can be used to define the first order effects. Based upon the examples above, Table 1 shows an example of how these effects can be defined as criteria for scoring purposes. If a long list of cyber-Events needs to be reduced to make the scoring process manageable, these impact criteria can be used to quickly prioritize the list to allow the team to focus on the top items. Any criteria developed for a CCE engagement should be relevant and appropriate for the organization. The following criteria are provided as examples that have been developed by electric sector subject matter experts (SMEs).

Area Impacted: Describes whether the impact of the attack scenario is geographically localized or if it impacts the entire system. Area impacted is described as a loss of load (both firm and supply) in this example, which can be translated into several affected endpoints or accounts.

Duration: Describes the length of an outage.

Attack Breadth: Describes the extent to which a targeted technology or system is deployed, resulting in adverse operational effects. The greater the span of impacted systems, the more difficult the restoration following an adverse Event.

It should be noted that in our example, attack breadth moves beyond the number of devices impacted, since this value also considers the additional resources needed for restoration, such as additional personnel or financial expenditures. For example, following a cyber-attack targeting advanced metering infrastructure (AMI), recovery efforts may be complicated by the quantity of field devices deployed.

Additional criteria can be identified to further refine the scoring. These criteria should relate to the entity’s values and primary concerns. Each should be clearly defined with thresholds that can be added to the previous criteria and used in Likert scale scoring.

Safety: Describes the potential impact on safety, including injuries requiring first aid or loss of life. For example, the power system outage resulted in health hazards or mortalities directly tied to the lack of available electric power. This value considers only the direct impacts to safety and not safety issues that stem from extended outages.

System Integrity Confidence: Describes whether restoration and recovery efforts can restore system integrity with confidence following an adverse Event (i.e., a system not operating as expected or intended, or, alternatively, malicious operation conducted by unauthorized users). One factor to consider is whether the initial attack propagates in multiple systems, therefore complicating restoration efforts. All of these may negatively impact an organization's confidence in their system.

Rather than focusing on the breadth of an attack, in some cases the system exploited may be central to the functionality of a critical service (i.e., the keep inside the castle). In these cases, an organization cannot operate the same system again because the risk of a follow-on attack is too high. In contrast, an organization may have confidence in their ability to replace impacted systems or devices and return to normal functionality and operation.

Cost (including restoration): This criterion considers the direct financial loss, including restoration costs, to the organization as a result of the failure scenario. Restoration cost is the cost to return the system to proper operation, not including any legal or other reparations as a result of the failure. It also includes secondary costs, such as purchasing replacement power in order to meet the need. For example, an organization with long term contracts will be impacted less than one with short term agreements.

It should be noted that the cost will be directly impacted by the size of an organization. That is, the cost of one cyber-Event may be evaluated as low for one utility but may be evaluated as medium for a smaller utility due to the greater "balance sheet" impact for the smaller utility.

Define Scoring Thresholds

This assessment is concerned with evaluating consequences. Once the criteria are decided upon, there needs to be a way to define the extent of their impact on the organization. The criteria are thus evaluated on a Likert scale, with values typically being none, low, medium, and high (numerical values 0, 1, 3, and 5, respectively). Referring to the criteria discussed above, the thresholds can be defined in the following manner (Table 1).

Table 1: Criteria scoring thresholds.

Criteria	None	Low	Medium	High
Area Impacted (Load or Customer Count)	Inconsequential	Loss of failure to service firm load of less than 300 MW (or) load supply loss of MSC or 2,000 MW, whichever is lower.	Loss of failure to service firm load between 301 and 1,500 MW (or) load supply loss of between 2,000 MW (or MSC, whichever is lower) and 3,000 MW	Loss of failure to service firm load greater than 1,500 MW (or) load supply loss of greater than 3,000 MW
Duration	Inconsequential	Return of all service in less than 1 day (inability to serve firm load) (or) supply outage for less than 1 week	Return to service in between 1 to 5 days (inability to serve firm load) (or) supply outage from 1 week to 1 month	Return to service in greater than or equal to 5 days (inability to serve firm load) (or) supply outage for greater than 1 month
Attack Breadth	Inconsequential	Elements of the system are vulnerable to an exploit that is actively being attacked and causing operational effects, but recovery is possible using immediately available resources. These events are covered within the utility's recovery plan.	Multiple system elements have the potential to be or have been successfully attacked causing operational effects. Recovery is possible but requires additional resources (i.e., time, personnel) not immediately available.	Many system elements have been successfully attacked causing operational effects. Restoration is complicated by the dispersed deployment of devices or scale. Timeline for recovery is unknown.
Safety	Inconsequential	Low but definite risk to safety, but only within the boundaries of "onsite."	There is a definite risk to safety "offsite," beyond the boundary of the fence.	There is a definite risk to safety that may include loss of life for one or multiple people, onsite or offsite.

System Integrity –Asset Owner Confidence	Inconsequential	Asset Owner has ability to restore and is confident in restoration integrity.	Asset Owner has knowledge to restore but does not have the resources (financial, time, personnel, etc.) to restore confidence in the system.	Asset Owner has ability to restore but is not confident of restoration integrity.
Cost	Inconsequential	The cost is significant, but well within the availability of an organization to recover from.	There is significant cost for recovery, and it will require multiple years for financial (balance sheet) recovery.	The cost triggers a liquidity crisis and potential result in the bankruptcy of the organization.

Determine Weighting Coefficients

The equation below is provided for calculating the scored impact points for each cyber-Event using the previously determined values.

$$\begin{aligned} &Scored\ Impact\ Points \\ &\qquad = \alpha(Area\ Impacted) + \beta(Duration) + \ \gamma(Attack\ Breadth) \\ &\qquad + \delta(System\ Integrity) + \varepsilon(Safety) + \zeta(Cost) \end{aligned}$$

Notice the weighting coefficient values (α, β, γ, δ, ε, and ζ) were determined by engineering and electric sector SMEs. However, these values can and should be altered to reflect the priorities of the subject organization. Typically, these weights are scaled 1-3, with 3 being reserved for the entity's primary concerns or values. For example, if an organization believes their primary concern is safety, then the value of ε can be increased so that ε has a value of 3.

In this example, the group agreed upon the following values for each weighting coefficient.

$$\begin{array}{lll} \alpha = 3 & \gamma = 3 & \varepsilon = 2 \\ \beta = 3 & \delta = 2 & \zeta = 1 \end{array}$$

Finalize Severity Scoring Matrix

To accommodate scoring by the CCE Team, an HCE Severity Scoring matrix is drafted from the combination of the established criteria, defined scoring thresholds, and the weighting coefficients. Table 2 provides an example with all elements present.

Table 2: HCE Severity Scoring matrix.

Criteria	None	Low	Medium	High
Area Impacted (Load or Customer Count) $\alpha = 3$	Inconsequential	Loss of failure to service firm load of less than 300 MW (or) load supply loss of MSC or 2,000 MW, whichever is lower.	Loss of failure to service firm load between 301 and 1,500 MW (or) load supply loss of between 2,000 MW (or MSC, whichever is lower) and 3,000 MW	Loss of failure to service firm load greater than 1,500 MW (or) load supply loss of greater than 3,000 MW
Duration $\beta = 3$	Inconsequential	Return of all service in less than 1 day (inability to serve firm load) (or) supply outage for less than 1 week	Return to service in between 1 to 5 days (inability to serve firm load) (or) supply outage from 1 week to 1 month	Return to service in greater than or equal to 5 days (inability to serve firm load) (or) supply outage for greater than 1 month
Attack Breadth $\gamma = 3$	Inconsequential	Elements of the system are vulnerable to an exploit that is actively being attacked and causing operational effects, but recovery is possible using immediately available resources. These events are covered within the utility's recovery plan.	Multiple system elements have the potential to be or have been successfully attacked causing operational effects. Recovery is possible but requires additional resources (i.e., time, personnel) not immediately available.	Many system elements have been successfully attacked causing operational effects. Restoration is complicated by the dispersed deployment of devices or scale. Timeline for recovery is unknown.

System Integrity—Asset Owner Confidence $\delta = 2$	Inconsequential	Asset Owner has ability to restore and is confident in restoration integrity.	Asset Owner has knowledge to restore but does not have the resources (financial, time, personnel, etc.) to restore confidence in the system.	Asset Owner has ability to restore but is not confident of restoration integrity.
Safety $\varepsilon = 2$	Inconsequential	Low but definite risk to safety, but only within the boundaries of "onsite."	There is a definite risk to safety "offsite." Beyond the boundary of the fence.	There is a definite risk to safety that may include loss of life for one or multiple people, onsite or offsite.
Cost $\zeta = 1$	Inconsequential	The cost is significant, but well within the availability of an organization to recover from.	There is significant cost for recovery, and it will require multiple years for financial (balance sheet) recovery.	The cost triggers a liquidity crisis and potential result in the bankruptcy of the organization.

The combination of the weighting coefficients and the severity threshold values will depend on each organization. For this matrix, the maximum number of impact points is 70. The total number of impact points is determined by multiplying each weighting coefficient by the highest score possible per criteria, and then adding the results together. The following equation demonstrates how the HCE Severity Score is calculated:

$$\begin{aligned} &Scored\ Impact\ Points \\ &= \alpha(Area\ Impacted) + \beta(Duration) + \gamma(Attack\ Breadth) \\ &+ \delta(System\ Integrity) + \varepsilon(Safety) + \zeta(Cost) \end{aligned}$$

$Maximum\ Impact\ Points$[b] $= \alpha(5) + \beta(5) + \gamma(5) + \delta(5) + \varepsilon(5) + \zeta(5)$

$$HCE\ Severity\ Score = \left(\frac{Scored\ Impact\ Points}{Maximum\ Impact\ Points}\right) * 100$$

[b] Note that not all organizations will assign the value of "5" to "High." As such, there is the potential the value for "Maximum Impact Points" will vary from organization to organization based not only on how many criteria are chosen, but also on the values they assign to their scoring definitions.

Scoring Example

As an example of the scoring process, the following HCE has been assessed and scored. The reasoning and results are shown in Table 3. The CCE Team consulted with SMEs in order to assess the impact of this Event. It should be noted that the cyber-Event scored describes a system failure rather than the outcome of a cyber-attack.

Example cyber-Event:

At the commissioning of an unspecified plant, a power interruption resulted in a loss of the control system. The plant had three combustion turbines (375 MW) and planned the construction of a 178 MW steam turbine to allow the plant to operate in combined cycle mode. As a result of the loss of power and resulting loss of the DCS, the auxiliary oil pump did not start after the trip. An emergency pump also did not start after the trip, and all lube oil was lost during roll down. The damage to the steam turbine was extensive and included damage to the bearings, the rotor, the inter-stage seals and blade, which resulted in a loss of $12 million in repairs and $30 million dollars in lost income.[i]

Table 3: HCE Severity Scoring example.

Criteria	None	Low	Medium	High
Area Impacted $\alpha = 3$		1 – While the cyber-Event does not describe the area impacted, the CCE Team assessed this cyber-Event as low due to the ability of the utility to serve load via alternative means.		
Duration $\beta = 3$				5 – The CCE Team believes that the resulting outage took more than 1 month to recover, given the amount of time required for the construction of the steam turbine.
Attack Breadth $\gamma = 3$			3– As described, the CCE Team believed that multiple systems could have been impacted (i.e., balance of plant [BOP] system, safety systems). Additionally, the impact could be applied to other facilities of the utility.	

System Integrity Confidence $\delta = 2$			3- While there is limited information, this cyber-Event would force the management of a utility to operate under the premise that their system integrity has been compromised (at least until a full cyber-forensics assessment can be conducted).	
Safety $\varepsilon = 2$		1 – There is a potential for a safety risk to onsite personnel.		
Cost $\zeta = 1$			3 – The cyber-Event describes a financial loss of $42 million. The CCE Team believed that this loss is significant, and it will require multiple years for financial recovery.	

Using the scoresheet above, the HCE Severity Score was calculated:

Recall:

$$\alpha(Area\ Impacted) + \beta(Duration) + \ \gamma(Attack\ Breadth) + \delta(System\ Integrity) + \varepsilon(Safety) + \zeta(Cost)$$

so

$$Scored\ Impact\ Points = \ 3(1) + 3(5) + 3(3) + 2(3) + 2(1) + 1(3) = 38$$

and

$$Maximum\ Impact\ Points = 3(5) + 3(5) + \ 3(5) + 2(5) + 2(5) + 1(5) = 70$$

thus

$$HCE\ Severity\ Score = \left(\frac{Scored\ Impact\ Points}{Maximum\ Impact\ Points}\right) * 100 = \left(\frac{38}{70}\right) * 100 = 54\%$$

It is important that all original documentation, including rationale, containing HCE Severity Scores be retained for future reference. Key decisions made by the CCE Team should also be documented and retained for future reference.

Scoring Lessons Learned

Limited Information

In evaluating various cyber-Events, the CCE Team may find they are unable to answer every question for every cyber-Event due to limited information. In these cases, some cyber-Events may be evaluated as less significant, due to their lower HCE Severity Scores. In order to compare these values against the others in the sample set, all scores should first be converted to percentages before being converted to percentiles.

Included in Table 4 is a description of how the HCE Severity Score can be adjusted in the event of imperfect information. Note that the maximum impact points will change as the CCE Team alters the weighting criteria. Using the values defined above in the example, the CCE Team may evaluate each scenario against a total of 70 potential impact points, with the most significant cyber-Events receiving higher scores. In cases where limited information required the elimination of a primary criterion (in this case duration, attack breadth, or area impacted), the total number of possible impact points decreases to 55.

For clarity, the second column was included to illustrate the elimination of some criteria (attack breadth, system integrity, or cost) for the example cyber-Event in this document. For each case, a percentage score was also calculated. While this method allows organizations to calculate HCE Severity Scores in limited information situations, it should be noted that eliminating criteria also decreases the validity of the HCE Severity Score for a given scenario.

Table 4: Example of readjusting scores based on imperfect information.

	Maximum Impact Points	**Scored Impact Points**	**HCE Severity Score**
No Criteria Eliminated	70	38	54%
One Primary Criterion Eliminated (i.e. Attack Breadth)	55	29	53%
One Secondary Criterion Eliminated (i.e. System Integrity)	60	32	53%
One Tertiary Criterion Eliminated (i.e. Cost)	65	35	54%

After calculating the HCE Severity Scores, identify the top HCE for further evaluation. If multiple HCEs are identified, some cyber-Events can be eliminated based on a predetermined threshold, as depicted in Figure 2.

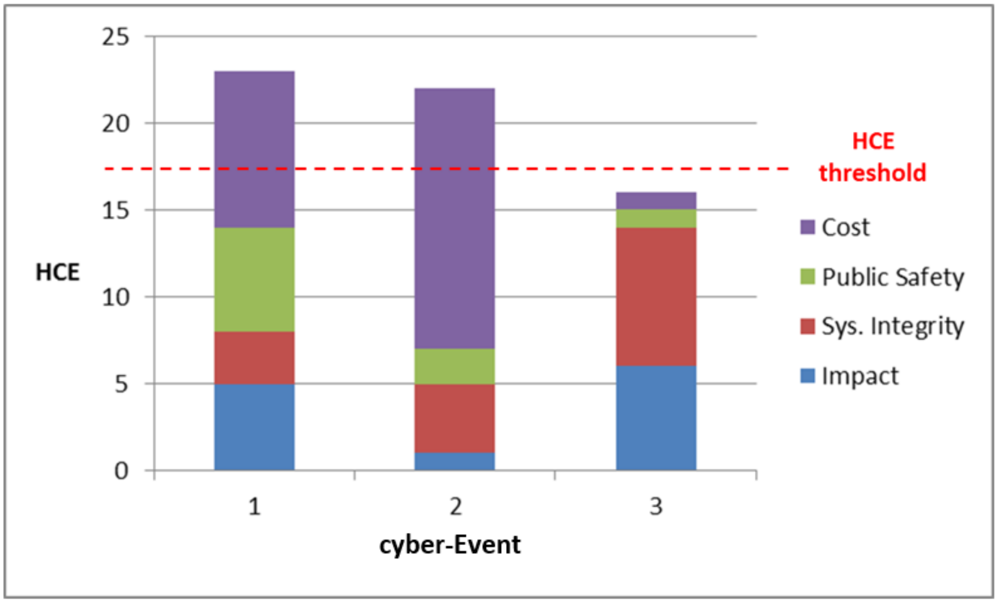


Figure 2: Example cyber-Events scored against a predetermined threshold.

Inconsistent Scoring

Each potential HCE may receive different scores from the various participants on the CCE Team. In this case, the team will need to look at the inconsistent scoring and hold a group conversation to discuss outliers to better understand the rationale for the scores given. This may cause cyber-Events to be scored and then revaluated. The team will need to decide how to incorporate these scoring changes and new rationale into the composite score. Regardless of the method chosen to combine the scores (i.e., median, average, most likely, point adjustment), care must be exercised to avoid inflating or deflating a potential cyber-Events final HCE Severity Score.

As stated previously, it is important that all original documentation, including rationale, concerning cyber-Event scoring be retained for future reference. This includes any actions taken by the CCE Team to handle scoring variance.

Revisiting Threshold Definitions and Weighting

After scoring multiple cyber-Events, the team may determine that all the scores are too similar, or that certain criteria are not given enough weight or do not provide value to the scoring process. When these situations arise, it is prudent to consider redefining, eliminating, or re-weighting the criteria to ensure that the process is functional. The CCE Team should discuss and document all changes and the rationale for those decisions.

The key takeaway is that the scoring process will likely encounter some difficulties; however, taking careful steps to correct these issues—while maintaining a group consensus—will be valuable time spent as the CCE Engagement progresses.

Validating Prioritized HCEs

After scoring is complete, the CCE Team will have identified the HCEs that are of greatest impact to the organization. This list should be prepared and presented to the entity's decision makers. This is done to validate that they agree with the group's findings and are willing to commit time and resources to the remaining CCE phases. This buy-in from the top is essential to avoid internal barriers or delays while accessing information, people, equipment, and processes necessary to conduct the engagement.

See Idaho National Laboratory's document titled "CCE Case Study: Ukraine Substation Power Outage" (INL-EXT-20-58092) for more Phase 1 examples on brainstorming Objective, Scope, Boundary Conditions, Events, cyber-Events, and criteria. The Ukrainian case study also demonstrates HCE scoring, validation, and prioritization.

[i] Wallace Ebner, "Strategies for the Prevention of Turbine Lube Oil System Failures," in *Proceedings of the ASME 2013 Power Conference*, July 29-August 1, 2013, Boston, MA.