IST-153 Workshop on Cyber Resilience

Assessing Cyber Resilience: Cyber Dependencies

Submitted by Argonne National Laboratory,
a U.S. Department of Energy National Laboratory
9700 S. Cass Avenue
Argonne, IL 60439
630-252-2000

Primary Author:
Nathaniel Evans
Global Security Sciences
Argonne National Laboratory
Argonne, Illinois 60439
Phone: 630-252-3733
Fax: 630-252-2964
nevans@anl.gov

Co-Author:
William Horsthemke
Global Security Sciences
Argonne National Laboratory
Argonne, Illinois 60439
Phone: 630-252-1605
Fax: 630-252-5128
horsthemke@anl.gov

The work described in this paper is cleared for public release.

The paper is technically correct.

This work was supported by the U.S. Department of Energy, Office of Science under contract DE-AC02-6CH11357.

The paper is NATO/PfP Unclassified.

The paper does not violate any proprietary rights.

Introduction

A cyber dependency is a connection between two assets, in which the state of one relies on that of the other. For example, in a networked business system, there may be many desktop computers linked to a central server and data-storage unit. These components depend on one another, and the loss of any one of them degrades the performance of the system as a whole.

Similarly, an industrial control process may involve sensors, data-acquisition computers, control-system computers, and servers, which operate together and must be linked to one another to provide effective monitoring and process control. Whenever separate components must operate together to complete a business function, there is a cyber dependency. Such dependencies must be identified and understood as part of a cyber resilience assessment.

What is a Cyber Dependency?

Identifying Cyber Dependencies

Cyber dependencies exist when computer systems depend upon other computer systems. Dependencies exist between multiple types of computer systems and include both information and services. Dependencies upon services range from information processing and storage to system configuration and security controls. Computers also depend upon networks to transmit data and upon specialized storage devices to store data; storage devices might require their own specialized communication networks.

An example of an internal dependency, or one that involves only organization-owned equipment, is that a computer that controls an industrial process might depend upon measurements provided by another computer. Thus, the process-control computer depends upon the measurement computer and upon the networks that allow the two computers to communicate.

External dependencies also appear, typically when organizations subscribe to specialized services provided by software or security vendors. For example, organizations often need to receive security updates, including operating system and application patches as well as anti-malware signatures, to maintain their security posture. This security requirement creates an external dependency not only on an external organization but also on the network infrastructure that enables the external communication.

Cyber dependencies are typically formed explicitly, such as the intentional dependency between an industrial control computer and a measurement computer. Other dependencies might form more implicitly, such as a measurement computer that receives its network settings at startup from a network configuration server. An implicit dependency may be hidden in the sense that the organization is not aware of it. Organizations typically recognize the critical cyber services that support or provide critical business functions, but these systems might depend upon other, less obvious cyber services. Because of this dependency, organizations should treat these supporting cyber services as essential systems and include them in their risk-management plan.

Characterizing Cyber Dependencies

Analysis of cyber dependency should consider the assets required —the end point systems— and the characteristics of the data dependency (for information or control). There are three possible states of data in a dependency relationship: data in motion, data at rest, and data in process. Understanding these data dependencies requires an analysis of the computer and network elements that are required for the transmission, storage, and processing of data.

Cyber Dependencies	
End Point Systems	End point systems characterize computer hardware devices (e.g., desktops, laptops, tablets) and their components.
Data in Motion	Data in motion characterizes data as they are in transit, including the processes and equipment (e.g., switches, networks, and firewalls) that are used for transfer of data.
Data at Rest	Data at rest characterizes data being physically stored, including storage capabilities and other storage device requirements.
Data in Process	Data in process (or data in use) characterizes data being edited or analyzed, including those by mainframes and clusters.

Assessing the Risk of Cyber Dependencies

Defining the Risk

Because the threats/hazards that affect any system or network element can propagate downstream to connected, dependent systems, risk analysis must consider not only a system's internal risk but also the risk of the upstream assets and of the transmission systems upon which it depends.

When assessing cyber dependencies, the analyst must consider the assets and their communication requirements, their data dependencies, the type of their data dependencies, and the type of security threats to which they might be vulnerable.

Four types of scenarios threaten the flow of data from the provider to the dependent asset. The data flow can be interrupted, intercepted, modified, or fabricated:

1. Flow interruption - when the data do not go to the receiver. The interruption thus affects data availability.
2. Flow interception - when the data are captured between the transmitter and the receiver. The interception thus affects data confidentiality.
3. Flow modification - when the data are processed (degraded) before reaching the receiver. The modification thus affects data integrity.
4. Flow fabrication - when the data that are received by the receiver are not originating from the good transmitter. The fabrication thus affects data authenticity.

The assessment should also evaluate whether the organization provides required services internally or if an external source provides said services. Note that a given service might depend upon both internal and external resources. For example, an offsite (internal) asset, which an organization owns, might communicate over an externally provided communication channel. The analysis should characterize the service provider (internal or external), operating environment, coupling and response behavior, type of failure, infrastructure characteristics, and state of operations.

Quantifying the Consequence of Loss

Four objective criteria help to quantify the consequence of losing a cyber service or one or more of its cyber dependencies:

1) Time before Impact Occurs
   An organization might not suffer immediately from the loss of a cyber service or its dependency. The impact might be delayed if the organization has a capacity to withstand the loss. Estimating the time before impact helps to quantify the consequence.

2) Extent of Impact
   The extent of impact can vary. Potential threats, including adverse physical events, can cause short-term interruptions, degradation of quality or integrity, or failure of a cyber dependency. Estimating the extent of impact should aim to measure the percentage of normal cyber functions that would be lost or degraded due to the potential threats. If measuring the percentage of loss is not feasible, the analyst can estimate the extent of impact in ordinal terms such as ‘severely’, ‘moderately’, or ‘minimally impacted’.

3) Degree of Dependency
   The reliance on a cyber dependency can vary. If the failure of a dependency directly causes the failure of an important cyber service or the business objective, then the dependency is high. If the failure of the dependency requires the organization to initiate its contingency plan or alternative measures, then the dependency is medium. If the organization can tolerate the failure of the dependency and continue to operate, then the dependency is low.

4) Time to Recover
   Consequence varies with the time to recover. The more quickly an organization recovers, the lower the consequence. With hot-standby, failover redundancy, an organization can tolerate loss. Without readily available recovery methods, the consequence of loss will increase.

The C-IST to Assess Cyber-Dependency Risk

As part of an overall assessment of cyber protection and resilience, the United States Department of Homeland Security (DHS) developed a cybersecurity assessment tool named the Cyber Infrastructure Survey Tool (C-IST). The C-IST evaluates cyber dependencies as part of an overall assessment of cyber protection and resilience. The methodology uses a survey to collect and inventory the attributes of an organization's cyber protection and resilience program.

The survey is a set of questions and answers that are designed to measure the attributes of cybersecurity. The attributes are scored by expert opinion and organized into five categories: (1) Cybersecurity Management, (2) Cybersecurity Forces, (3) Cybersecurity Controls, (4) Incident Response, and (5) Dependencies.

Expert opinion is elicited to measure the relative importance and contribution of each category and of each of the question sets within the categories. By combining the relative importance of all of the attributes of cybersecurity, the methodology creates a composite index (the Cyber Protection and Resilience Index, or CPRI) that reflects the relative effectiveness of an organization's cyber protection and resilience program as compared to that of other organizations with similar critical cyber services (CCSs).

Through the C-IST survey process, an organization identifies its CCSs, characterizes its dependencies, and identifies the relevant threat scenarios as described above. To quantify the impact of losing dependencies, the C-IST asks specific questions about each type of dependency. If the dependency is lost, what is percentage loss or degradation of normal functionality? How long before the impact occurs? How long the organization can continue to operate (survive) after suffering the loss or degradation of normal functionality?

To assess the ability to withstand or recover from the loss, the C-IST asks whether other options are available to fulfill the role of the lost dependency and how much time is required to employ those recovery options. The options vary from redundant equipment and data pathways to alternative processes and procedures.

Dependency Curves to Visualize the C-IST
After quantifying the severity, immediacy, and survivability of the impact of losing their cyber dependencies, the organization can use dependency curves to visualize the effect of losing a dependency over time. Figure 1 below illustrates an example of a dependency curve:

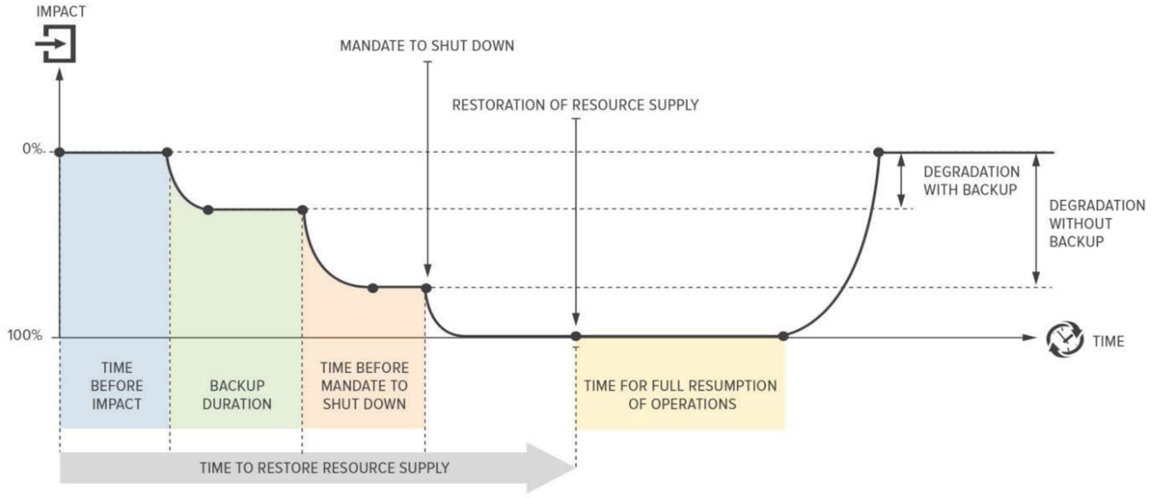
IMPACT
MANDATE TO SHUT DOWN
RESTORATION OF RESOURCE SUPPLY
0%
DEGRADATION WITH BACKUP
DEGRADATION WITHOUT BACKUP
100%
TIME
TIME BEFORE IMPACT
BACKUP DURATION
TIME BEFORE MANDATE TO SHUT DOWN
TIME FOR FULL RESUMPTION OF OPERATIONS
TIME TO RESTORE RESOURCE SUPPLY

Figure 1: Dependency Curve

The dependency curve starts when the loss occurs, and the blue region shows how long before the impact has its effect. The green period depicts the reduction or degradation in service that the impact causes. During this period, the organization also relies upon backup operations, if available. If the backup operations fully replace the lost service, the green period remains steady at 0% loss of service.

The pink period shows the continued degradation of service until the organization must shut down operations. The dependency curve remains constant during this period if the backup systems remain fully operational.

The curve next depicts the full outage (blank) and the restoration (orange) periods, followed by the actual resumption of full service.

Managing the Risk of Cyber Dependencies

The relationship that is formed by a dependency requires special attention because it might pose a trust-based security risk and may be difficult to monitor. For example, an organization might relax security controls or grant special permissions to allow communication between devices that a dependency may require. Granting special permissions forms a trust between the elements that might permit the transmission of threats. Organizations must assess these security risks and determine whether they should add controls to mitigate the risk that this trusted relationship poses.

The organization must monitor the dependency to detect threats and evaluate uptime, as the dependency might create an attackable opening. Because the organization needs to use the dependency, the monitor should understand how to measure whether the dependency is operating as expected. If the monitor detects problems, he or she should provide information on the type and source of each issue.

When problems with cyber dependencies occur, the organization needs a contingency plan that addresses how to respond and recover. When developing the contingency plan, the organization should evaluate whether the recovery time of the dependencies meets the organization’s recovery time requirements. If not, the organization should consider alternative recovery strategies such as provisioning redundant systems. Redundant systems vary in cost and complexity, ranging from spares on a shelf to fully provisioned, hot-standby, redundant components with automated failover.

The cyber elements used in cyber dependencies might require special configurations or use specialized software and hardware. The plan should address how to acquire and configure replacement elements. Some specialized elements, such as control systems, might have reached end-of-life which will require the organization to develop a plan to find and configure suitable replacements.

The contingency plan should also address, if possible, the use of alternatives other than cyber elements. For example, some computerized control systems permit manual control.

In addition to preparing for the loss of internal dependencies, the contingency plan should address the potential loss of external dependencies (if the organization requires them). The organization must to ensure that its external partner has a recovery or restoration plan that meets its own requirement. If not, the organization should develop its own alternative.

Conclusion

Critical business functions often depend upon cyber systems, and organizations typically recognize the critical cyber services that support or provide these functions. However, organizations might not recognize the elements upon which those critical cyber services depend.

Critical cyber services often depend upon other elements, and the degree of dependency varies widely. Sometimes the business function depends only partially on a cyber service, but sometimes the function requires one or more cyber elements. Sometimes multiple cyber elements depend upon each other such that the loss of one might cause the loss of many or all. Dependencies can span locations or cross-organizational boundaries. An organization might own and control all of its dependencies, but it might depend upon external providers, either for a particular service or for a communication path.

Organizations must understand when and how they should respond to the loss or degradation of their crucial cyber elements and must ensure that they can detect the loss of a dependency and the impact of that loss. Listed below are the key steps in managing cyber dependencies:

1) Identify the critical cyber services (CCSs) upon which the organization depends
2) Identify the cyber dependencies of those CCSs and their cyber components
    a) Assess the relative importance of the CCSs and their cyber components
3) Characterize each cyber dependency
    a) Determine whether the organization owns and controls the cyber dependency components or whether it depends upon an external organization
    b) If it is external, evaluate whether the external organization has sufficient protection and recovery procedures to maintain it
    c) Quantify the consequence of its loss: the extent of impact and the time before impact
    d) Define its type and the treats it faces
        i) Flow interruption, interception, modification, and/or fabrication
    e) Evaluate its vulnerabilities
4) Evaluate how the organization manages the risk of its cyber-dependency components
    a) Assess whether the organization sufficiently monitors the performance of the cyber dependency
    b) Assess how quickly the organization can recover the lost cyber dependency
    c) Measure whether the organization can recover before serious harm occurs
    d) Assess whether the organization can restore the cyber dependency