CIS Control 11: Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Why is this CIS Control Critical?

In the cybersecurity triad -- Confidentiality, Integrity, and Availability (CIA) -- the availability of data is, in some cases, more critical than its confidentiality. Enterprises need many types of data to make business decisions, and when that data is not available or is untrusted, then it could impact the enterprise. An easy example is weather information to a transportation enterprise.

When attackers compromise assets, they make changes to configurations, add accounts, and often add software or scripts. These changes are not always easy to identify, as attackers might have corrupted or replaced trusted applications with malicious versions, or the changes might appear to be standard-looking account names. Configuration changes can include adding or changing registry entries, opening ports, turning off security services, deleting logs, or other malicious actions that make a system insecure. These actions do not have to be malicious; human error can cause each of these as well. Therefore, it is important to have an ability to have recent backups or mirrors to recover enterprise assets and data back to a known trusted state.

There has been an exponential rise in ransomware over the last few years. It is not a new threat, though it has become more commercialized and organized as a reliable method for attackers to make money. If an attacker encrypts an enterprise's data and demands ransom for its restoration, having a recent backup to recover to a known, trusted state can be helpful. However, as ransomware has evolved, it has also become an extortion technique, where data is exfiltrated before being encrypted, and the attacker asks for payment to restore the enterprise's data, as well as to keep it from being sold or publicized. In this case, restoration would only solve the issue of restoring systems to a trusted state and continuing operations. Leveraging the guidance within the CIS Controls will help reduce the risk of ransomware through improved cyber hygiene, as attackers usually use older or basic exploits on insecure systems.

11.1: Establish and Maintain a Data Recovery Process

Establish and maintain a documented data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Documentation	Govern	1, 2, 3

Dependencies

- None

Inputs

1. Data recovery process for the enterprise
2. Date of last update to the data recovery process

Operations

1. Check if the enterprise has a data recovery process Input 1
    1. If so, M1 = 1
    2. If not, M1 = 0
2. Examine the enterprise's data recovery process and determine if it addresses, at a minimum, the scope of data recovery activities, recovery prioritization, and the security of backup data
    1. For each element included within the process, assign the element a value of
        1. M2 = sum of all the values.
3. Compare the date of the last update to the data recovery process to the curren date and capture the timeframe in months (M3)

Measures

- M1 = Output of Operation 1
- M2 = Sum of elements included in the data recovery process
- M3 = Timeframe in months of the last update to the data recovery process

Metrics

- If M1 is 0, the Safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve, this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	**The percentage of elements included in the data recovery process**
Calculation	`M2 / M3`

11.2: Perform Automated Backups

Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.

Asset Type	**Security Function**	**Implementation Groups**
Data	Recover	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory
3. `GV3`: Configuration standards

Operations

1. For each asset in `GV1` identify and enumerate assets that are in-scope for automated backups: `GV33` (M1)

2. Use `GV5` to identify authorized backup software and for each asset identified in Operation 1

    1. Identify and enumerate assets covered by at least one authorized backup software: `GV34` (M2)
    2. Identify and enumerate assets not covered by at least one authorized backup software (M3)

3. Use `GV3` to check if the software on assets identified in Operation 2.1 is configured correctly

    1. Identify and enumerate assets with properly configured backup software (M4)
    2. Identify and enumerate assets with improperly configured backup software (M5)

4. For each asset with backup software identified in Operation 2.1, examine logs to determine the most recent successful backup date. Compare that date to the current date and capture the timeframe in days.

    1. Identify and enumerate assets that have been backup within seven days or less (M6)
    2. Identify and enumerate assets that have been backed up outside of a seven-day window (M7)

Measures

- M1 = Count of assets within scope for automated backups
- M2 = Count of in-scope assets with authorized backup software installed
- M3 = Count of in-scope assets without authorized backup software installed
- M4 = Count of in-scope assets with properly configured backup software
- M5 = Count of in-scope assets with improperly configured backup software
- M6 = Count of in-scope assets backed up within a week
- M7 = Count of in-scope assets not backed up within a week

Metrics

Coverage

Metric	**The percentage of in-scope assets with properly configured authorized backup software**
Calculation	`M4 / M1`

Compliance

Metric	**The percentage of in-scope assets backed up within a week timeframe**
Calculation	`M6 / M1`

11.3: Protect Recovery Data

Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

Asset Type	Security Function	Implementation Groups
Data	Protect	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV33`: Assets that are in-scope for automated backups
2. `GV34`: Assets with authorized backup software installed
3. `GV3`: Configuration Standard

Operations

1. For each asset with backup software installed, use `GV3` to check if encryption is configured for backups

    1. Identify and enumerate assets with software configured to encrypt backups (M2)
    2. Identify and enumerate assets with software not configured to encrypt backups (M3)

Measures

- M1 = Count of Input 1: `GV33`
- M2 = Count of software configured to encrypt backups
- M3 = Count of software not configured to encrypt backups

Metrics

Coverage

Metric	The percentage of in-scope assets with backup software properly configured to encrypt backups
Calculation	`M2 / M1`

11.4: Establish and Maintain an Isolated Instance of Recovery Data

Establish and maintain an isolated instance of recovery data. Example implementations include, version-controlling backup destinations through offline, cloud, or off-site systems or services.

Asset Type	Security Function	Implementation Groups
Data	Recover	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV33`: Assets that are in-scope for automated backups
2. `GV34`: Assets with authorized backup software installed
3. `GV3`: Configuration standards

Assumptions

Configuration for backups will contain information about the destination of backups

Operations

1. For each asset in Input 2 `GV34`, use configuration standards in `GV3` to check the destination of backups
    1. Identify and enumerate assets properly configured to send backups to an isolated instance (M2)

2. Identify and enumerate assets not properly configured to send backups to an isolated instance (M3)

Measures

- M1 = Count of Input 1 `GV33`
- M2 = Count of assets with backups sent to an isolated instance
- M3 = Count of assets with backups not sent to an isolated instance

Metrics

Coverage

Metric	**The percentage of assets configured to send backups to an isolated instance**
Calculation	`M2 / M1`

11.5: Test Data Recovery

Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

Asset Type	Security Function	Implementation Groups
Data	Recover	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Inputs

1. Current set of backups for the enterprise
2. Date of last backup recovery test

Assumption

1. Enterprise will know what a properly working restored backup looks like.

Operations

1. Use Input 1 to restore a sampling of the backups to a temporary location

    1. Enumerate the total number of backups restored (M1)
    2. Identify and enumerate backups that are properly working after being restored (M2)

3. Identify and enumerate backups that did not properly work after being restored (M3)

2. Compare Input 2 to the current date and capture the time frame in months (M4)

Measures

- M1 = Count of backups being tested
- M2 = Count of properly working backups after restoration
- M3 = Count of backups not properly working after restoration
- M4 = Timeframe between tests of backup recovery

Metrics

- If M4 is greater than three months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Backup Integrity Quality

Metric	**The percentage of restored backup sampling deemed to be properly working**
Calculation	`M2 / M1`