CIS Control 17: Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Why is this CIS Control Critical?

A comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. Often, the final two get overlooked in immature enterprises, or the response technique to compromised systems is just to re-image them to their original state and move on. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern.

We cannot expect our protections to be effective 100% of the time. When an incident occurs if an enterprise does not have a documented plan -- even with good people -- it is almost impossible to know the right investigative procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover.

Along with detection, containment, and eradication, communication to stakeholders are key. If we are to reduce the probability of material impact due to a cyber event, the enterprise's leadership must know what potential impact there could be, so that they can help prioritize remediation or restoration decisions that best support the enterprise. These business decisions could be based on regulatory compliance, disclosure rules, service-level agreements with partners or customers, revenue, or mission impacts.

Dwell time from when an attack happens to when it is identified can be days, weeks, or months. The longer the attackers are in the enterprise's infrastructure, the more embedded they become, and they will develop more ways to maintain persistent access for when they are eventually discovered. With the rise of ransomware, which is a stable moneymaker for attackers, this dwell time is critical, especially with modern tactics of stealing data before encrypting it for ransom.

17.1: Designate Personnel to Manage Incident Handling

Designate one key person, and at least one backup, who will manage the enterprises incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach. If using a service provider, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Users	Respond	1, 2, 3

Dependencies

- None

Inputs

1. `GV51`: Enterprise Incident Response Documentation
2. Date of last update or review of the documentation

Operations

1. Determine whether the enterprise documents designated personnel to manage incident handling by reviewing Input 1 `GV51`. Input 1 can be an incident response plan or other documentation.

    1. If documentation designating personnel exists, M1 = 1
    2. If documentation designating personnel does not exist, M1 = 0

2. Determine whether the documentation, at a minimum, outlines the following components: primary personnel, backup personnel, roles and responsibilities of each

    1. For each component included, assign a value of 1. Sum the values. (M2)

3. Compare Input 2 to the current date and capture the timeframe in months (M3)

Measures

- M1 = Output of Operation 1
- M2 = Count of components included for designated personnel documentation
- M3 = Timeframe since the last update or review of documentation in months

Metrics

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

Completeness

Metric	**The percentage of components included in the documentation for designated incident handling personnel**
Calculation	`M2 / 3`

17.2: Establish and Maintain Contact Information for Reporting Security Incidents

Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.

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

Dependencies

- None

Inputs

1. GV51: Enterprise Incident Response Documentation
2. Date of last update or review of the documentation

Operations

1. Determine whether the enterprise documents establish and maintain contact information for reporting security incidents by reviewing Input 1 GV51. Input 1 can be an incident response plan or other documentation.
    1. If documentation outlining contact information exists, M1 = 1
    2. If documentation outlining contact information does not exist, M1 = 0
2. Compare Input 2 to the current date and capture the timeframe in months (M2)

Measures

- M1 = Output of Operation 1
- M2 = Timeframe since the last update or review of documentation in months

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M2 is greater than twelve months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

17.3: Establish and Maintain an Enterprise Process for Reporting Incidents

Establish and maintain an documented enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review 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. `GV51`: Enterprise Incident Response Documentation
2. Date of last update or review of the documentation

Operations

1. Determine whether the enterprise documents process for reporting incidents by reviewing Input 1 `GV51`. Input 1 can be an incident response plan or other documentation.
    1. If documentation for reporting incidents exists, M1 = 1
    2. If documentation for reporting incidents does not exist, M1 = 0
2. Determine whether the documentation, at a minimum, outlines the following components: reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported
    1. For each component included, assign a value of 1. Sum the values. (M2)
3. Compare Input 2 to the current date and capture the timeframe in months (M3)
4. Determine whether the process documentation is available to the whole workforce
    1. If it is available to all, M4 = 1
    2. If it is not available to all, M4 = 0

Measures

- M1 = Output of Operation 1
- M2 = Count of components included for reporting incidents process documentation
- M3 = Timeframe since the last update or review of documentation in months
- M4 = Output of Operation 4

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M3 is greater than twelve months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.
- If M4 is 0, this Safeguard receives a failing score for this metric. Other metrics still apply.

Completeness

Metric	The percentage of components included in the documentation for designated incident handling personnel
Calculation	`M2 / 4`

17.4: Establish and Maintain an Incident Response Process

Establish and maintain a documented incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Documentation	Govern	2, 3

Dependencies

- None

Inputs

1. `GV51`: Enterprise Incident Response Documentation
2. Date of last update or review of the documentation

Operations

1. Determine whether the enterprise documents an incident response process: `GV52` by reviewing Input 1 `GV51`. Input 1 can be an incident response plan or other documentation.
    1. If the documentation for an incident response process exists, M1 = 1
    2. If the documentation for an incident response process does not exist, M1 = 0
2. Determine whether the documentation, at a minimum, outlines the following components: roles and responsibilities, compliance requirements, and a communication plan
    1. For each component included, assign a value of 1. Sum the values. (M2)
3. Compare Input 2 to the current date and capture the timeframe in months (M3)

Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the incident response process documentation
- M3 = Timeframe since the last update or review of documentation in months

Metrics

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

Completeness

Metric	**The percentage of components included in the documentation for designated incident handling personnel**
Calculation	`M2 / 3`

17.5: Assign Key Roles and Responsibilities

Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Users	Respond	2, 3

Dependencies

- Safeguard 17.4: Establish and Maintain an Incident Response Process

Inputs

1. `GV52`: Incident response process
2. Date of last update or review of the documentation

Operations

1. Determine whether the enterprise documents key roles and responsibilities by reviewing Input 1 `GV52`

    1. If documentation exists, M1 = 1
    2. If documentation does not exist, M1 = 0

2. Using the documentation in Input 1 `GV52`, identify and enumerate the roles and responsibilities (M2)

3. For each role and responsibility identified in Operation 2, determine whether an individual is mapped to that role and responsibility

    1. Identify and enumerate those that are mapped (M3)
    2. Identify and enumerate those that are not mapped (M4)

4. Compare Input 2 to the current date and capture the timeframe in months (M5)

Measures

- M1 = Output of Operation 1
- M2 = Count of roles and responsibilities outlined in the process
- M3 = Count of roles and responsibilities that are mapped to an individual
- M4 = Count of roles and responsibilities that are not mapped to an individual
- M5 = Timeframe since the last update or review of documentation in months

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M5 is greater than twelve months, then this Safeguard is measured at a 0 and receives a failing score. The other metrics don't apply.

Completeness

Metric	**The percentage of roles and responsibilities that are mapped to an individual**
Calculation	`M3 / M2`

17.6: Define Mechanisms for Communicating During Incident Response

Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, secure chat, or notification letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Users	Respond	2, 3

Dependencies

- Safeguard 17.4: Establish and Maintain an Incident Response Process

Inputs

1. `GV52`: Incident response process
2. Date of last update or review of the documentation

Operations

1. Determine whether the enterprise document mechanisms for communication by reviewing Input 1 `GV52`

    1. If the documentation for an incident response process exists, M1 = 1
    2. If the documentation for an incident response process does not exist, M1 = 0

2. Determine whether the documentation, at a minimum, outlines primary and secondary mechanisms for communication

    1. For each mechanism included, assign a value of 1. Sum the values. (M2)

3. Compare Input 2 to the current date and capture the timeframe in months (M3)

Measures

- M1 = Output of Operation 1
- M2 = Count of mechanisms for communication included in the documentation
- M3 = Timeframe since the last update or review of documentation in months

Metrics

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

Completeness

Metric	**The percentage of components included in the documentation for designated incident handling personnel**
Calculation	`M2 / 2`

17.7: Conduct Routine Incident Response Exercises

Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision-making, and workflows. Conduct testing on an annual basis, at a minimum.

Asset Type	Security Function	Implementation Groups
Users	Recover	2, 3

Dependencies

- Safeguard 17.4: Establish and Maintain an Incident Response Process

Inputs

1. GV52: Incident response process
2. Date of last exercise or test

Operations

1. Determine whether the enterprise's incident response process includes routine incident response exercises by reviewing Input 1 GV52
    1. If the documentation includes exercises, M1 = 1
    2. If the documentation does not include exercises, M1 = 0
2. Determine whether the documentation for exercises, at a minimum, outlines test communication channels, decision-making, and workflows
    1. For each mechanism included, assign a value of 1. Sum the values. (M2)
3. Compare Input 2 to the current date and capture the timeframe in months (M3)

Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the documentation
- M3 = Timeframe since the last exercise or test in months

Metrics

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

Completeness

Metric	**The percentage of components included in the documentation for incident response exercises**
Calculation	M2 / 3

17.8: Conduct Post-Incident Reviews

Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

Asset Type	Security Function	Implementation Groups
Users	Recover	2, 3

Dependencies

- Safeguard 17.4: Establish and Maintain an Incident Response Process

Inputs

1. `GV52`: Incident response process
2. Last post-incident review

Operations

1. Determine whether the enterprise's incident response process includes post-incident reviews by reviewing Input 1 `GV52`
    1. If the documentation includes post-indecent reviews, M1 = 1
    2. If the documentation does not include post-incident reviews, M1 = 0
2. Use Input 2 to determine if post-incident reviews include, at a minimum, the following components: lessons learned and follow-up actions
    1. For each component included, assign a value of 1. Sum the values. (M2)

Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the documentation

Metrics

- If M1 is 0, this safeguard receives a failing score. The other metrics don't apply.

Completeness

Metric	**The percentage of components included in post-incident reviews during Incident response exercises**
Calculation	`M2 / 2`

17.9: Establish and Maintain Security Incident Thresholds

Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include abnormal activity, security vulnerability, security weakness, data breaches, privacy incidents, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Documentation	Recover	3

Dependencies

- Safeguard 17.4: Establish and Maintain an Incident Response Process

Inputs

1. `GV52`: Incident response process
2. Date of last update or review of the documentation

Operations

1. Determine whether the enterprise documents security incident threshold by reviewing Input 1 `GV52`

    1. If the documentation for a security incident threshold exists, M1 = 1
    2. If the documentation for a security incident threshold does not exist, M1 = 0

2. Determine whether the documentation, at a minimum, outlines the following components: differentiates between incident and event, prioritization schema based on known or potential impact, procedure relying on this schema is used to determine status update frequency during incident handling, and procedure relying on this schema is used to determine escalation paths during incident handling

    1. For each mechanism included, assign a value of 1. Sum the values. (M2)

3. Compare Input 2 to the current date and capture the timeframe in months (M3)

Measures

- M1 = Output of Operation 1
- M2 = Count of components included in the documentation
- M3 = Timeframe since the last update or review of documentation in months

Metrics

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

Completeness

Metric	**The percentage of components included in the documentation for security incident thresholds**
Calculation	`M2 / 4`