

Ransomware

ICS4ICS Procedure Template

|  |
| --- |
| Instructions The following are suggestions about how you can update this template to create a procedure for your company:   * Identify the roles required on the Decision Team that will manage Ransomware decisions * Review and update the Decision Considerations based on your company requirements * Test this Ransomware Procedure and update as appropriate |
| DisclaimerISA, ISAGCA, and the ICS4ICS Program provide this template to help asset owners create procedures to perform ICS4ICS and/or Cyber Incident Response and/or other related tasks. Each Asset Owners must update this template based on the needs of their company and ensure the procedure is review and approved by the appropriate parties (e.g., legal, senior management, corporate governance, government relations, etc.) from within their company. |

## Purpose

This document is intended to provide information to describe how <<company>> will manage ransomware.

## Situation Trigger

Ransomware has been detected on company system(s) or a ransomware demand has been made requesting payment to unlock systems.

## Symptoms

IT and/or OT systems are locked, and normal procedures have not worked to remove the ransomware and recovery of the impacted IT and/or OT Systems appears lengthy or not possible or unknown

## Escalation

If the ransomware cannot be removed, normal escalation procedures will be used which results in notification to an authorized Incident Commander

## Declaration

The Incident Commander will declare an Incident, if appropriate

## Decision Team

The following parties will be engaged to assess the situation, make decisions, and determine next steps:

* Incident Commander
* Operations Section Chief
* Intelligence Officer (potentially, a mutual aid providers)
* Safety Officer
* Technical Representative familiar with impacted systems (e.g., Plant Engineering)
* Corporate Cyber Security
* Corporate Legal and outside council
* Government Relations
* Cyber Insurance Representative if you have insurance
* Public Information Officer
* FASC and/or other from Finance and/or Corp Audit
* Privacy expert if there is any potential impact on the release or compromise of personal data
* NOTE: Crisis Management Team (CMT) is the final authority to make decisions

## Decision Process

The Decision Team will consider the following factors to make decisions about the ransomware:

* Assess Legal Ransomware Restrictions or requirements (e.g., an assessment must be completed previously, and a table created describing laws or regulations that impact ransomware payments)
* Review Corporate Policies (e.g., an assessment must be completed previously, and a table create summarizing any Corporate Policies that may impact how we handle ransomware requests)
* Assess the impact from the ransomware:
  + Life Safety risks
  + Environmental impact and Protection
  + Business and Financial impact (thresholds of impact may be defined at a company-wide/corporate level)
  + Impact to communications and other IT services from the ransomware (the enterprise network and systems may be impacted)
* Assess the recovery options
  + Consider BCP capabilities to manually operate or leverage redundant systems and DR capabilities to recover systems (e.g., recovery tiers: manual operations, automated operations, optimized operations)
* Consider the magnitude and possible alternatives to recovery from ransomware based on an IT/OT Technical Assessment
  + Stabilize (Isolate/Contain) the Incident within a single system or network
* Understand likelihood of payment working
  + Potential deadline imposed by ransomware
  + Understand the ransomware threat actors better and the likelihood they will provide the key to remove the ransomware on your systems; This is an example of a company that provides those services: <https://www.coveware.com/>
* Communication Strategy (how do we get ahead of this in the media/public perception is a potential problem)
* Understand Government Reporting Requirement (e.g., an assessment must be completed previously, and a table created describing government reporting requirements)
* Identify ransomware approval processes (e.g., identify who must approve ransomware payments and ensure they have sufficient Delegation of Authority)

## Decision Factors (Table)

The Decision Team will consider the following factors to make decisions about the ransomware:

|  |  |  |
| --- | --- | --- |
| Type | Enforcement | Description |
| Law | Required | <describe each law that impacts decisions> |
| Regulation | Required | <describe each regulation that impacts decisions> |
| Reporting | Required | <describe each reporting law that impacts decisions> |
| Reporting | Recommended | <describe each reporting recommendation that impacts decisions> |
| Insurance | Input | <describe the company insurance policy and how it typically covers Ransomware> |
| Corp Policy | Required | <describe each Corp Policy requirement that impacts decisions> |
| Corp Policy | Recommended | <describe each Corp Policy recommendation that impacts decisions> |
| Company Standard | Required or recommended | <describe each company standard that is required or recommended that impacts decisions> |
| IT/OT Technical Assessment | Real-time Input | Review the IT/OT Technical Assessment data provided by staff periodically |
| Decision Approval | Required | <describe company decision processes required to finalize decisions> |

## IT/OT Technical Assessment (on-going)

After Event (incident) Escalation, the IT and/or OT staff continue to assess alternatives to resume normal operations which may include:

* Capture an image of the impacted systems, if possible (e.g., try to take a copy of the impacted systems, logs, and other related files)
* Assess and document the impact the ransomware is having on operations (e.g., shutdown, partially disabled, impact to other operational units)
* Determine the potential risk to other industrial operations and take appropriate steps to protect them (e.g., network separation, shutdown) – See Network Separation / Shutdown Procedure
* Identify alternatives to remove the ransomware (e.g., leverage information from government sites or paid or unpaid resources)
* Estimate the Recovery Time (hours, days) needed to restore these systems (e.g., rebuild from backups using Disaster Recovery procedures)
* Evaluate data required to perform forensics to determine if it is still available or it has been impacted by the ransomware (e.g., review log data, SIEM, IDS, EDR, and other system data)
* Begin forensics activities – If needed engage the appropriate parties (e.g., a mutual aid partner should have already been selected and under contract, if this function is not done by company staff)
  + NOTE: Legal staff should provide language informing staff and mutual aid partner staff that the company retains “attorney client privilege” which means that no one can force individuals to disclose in court what they tell each other as part of their work. Everyone needs to understand that the privilege belongs to the company, not to staff personally.
* Recommend a mutual aid partner who can assist with the assessment and remediation of the ransomware (e.g., Dragos, Mandiant, etc.)
* Periodically, document your finding and share with the Incident Commander