****

 **Ransomware incident response plan template**

| **Section** | **Title** | **Description** | **Completed** |
| --- | --- | --- | --- |
| 1 | Introduction, policy and organization | * Specify the purpose, scope, goals and objectives of the ransomware incident response plan.
* Identify any regulations or statutes that govern the plan (e.g., FEMA, OSHA, local code).
* List who will have hard copies of the plan and who will have access to the plan electronically.
* Include a schedule of plan revisions.
* Include management approvals and authorizations.
 | [ ]  |
| 2 | Incident management strategy | * Define the approach to managing a ransomware attack, for example, isolate the malware, remain at office, work remotely.
* Identify alternate resources and supply sources.
* Identify resources to back up systems, data, databases and other critical information assets.
* Define incident response team roles and responsibilities during and after an event.
* Establish lines of authority in a ransomware attack.
* List people who can back up primary team members if they are unavailable.
* Document actions to take when responding to ransomware activities.
 | [ ]  |
| 3 | Incident response communications | * Define who is to be contacted during the incident.
* Determine the sequence and frequency of messages to management, employees and others.
* Prepare a detailed contact list with all methods of reaching team members, key vendors, law enforcement, first responders and other government agencies.
* Include roles and responsibilities in contact lists.
* Deploy conference technologies to ensure employees can keep in touch with managers and team members.
 | [ ]  |
| 4 | Media management | * Prepare contact details for external contacts, including stakeholders, vendors and supply chain members.
* Establish guidelines for managing the media during and after the event.
* Prepare statements for delivery to the media.
* Identify primary and alternate media contacts.
* Provide training to internal media contacts on how to deal with the media.
* Set up a meeting place for media briefings.
* Train employees on how to interact with the media, if this is permitted.
* Establish protocols to manage employee use of social media during a ransomware incident.
 | [ ]  |
| 5 | Incident response procedures | * Examine attack data from firewalls, intrusion detection equipment and antimalware software.
* If the incident assessment indicates a ransomware attack, convene the incident response team.
* Isolate the malware for further analysis.
* Examine communications from the attack perpetrators to see what they want.
* Determine initial steps to mitigate the severity of the attack, e.g., use software to examine the malware attack signature and identify possible remedies.
* Proceed with steps to identify what has been compromised and to regain access.
* Determine initial steps for managing how the company operates during the incident.
* Schedule regular team meetings to assess progress.
* Communicate status regularly to employees, management, stakeholders and the media.
* Continue with steps to isolate and mitigate/eliminate the malware.
* If response actions are unsuccessful, discuss options with incident response team and senior management.
* Once the situation has been remedied, compile notes on attack activity in preparation for a post-event review and after-action report.
 | [ ]  |
| 6 | Conduct a post-event review and prepare a report | * Gather output data from firewalls, intrusion detection equipment and antimalware software for further analysis.
* Examine reporting from systems dealing with the ransomware attack; identify what worked and what did not work.
* Discuss next steps, including updating cybersecurity plans and ransomware incident response plans, updating cybersecurity prevention tools, etc.
* Perform follow-up tests of antimalware prevention software and test updated ransomware plans.
* Initiate a plan to complete remediation steps identified and perform tests to validate corrections are appropriate.
* Prepare an after-action report for presentation to senior management on the incident.
* Monitor all possible malware entry points and monitor systems and data that could be affected in the future.
 | [ ]  |
| 7 | Link with other emergency plans | * Determine if activation of other plans, such as business continuity plans, is needed.
* If this is the case, determine when one plan ends and another is activated.
 | [ ]  |
| 8 | Awareness and training | * Develop and conduct training programs for incident response team members.
* Develop and conduct training programs for senior management and all employees.
* Create an awareness program to keep employees, management and stakeholders aware of the ransomware incident response plan.
 | [ ]  |
| 9 | Plan exercising | * Schedule and conduct periodic exercises of the ransomware incident response plan, including tabletop walkthroughs and full active simulations involving activation of the incident response team and other third-party organizations.
* Update the incident response based on exercise results.
 | [ ]  |
| 12 | Plan review, audit and maintenance | * Establish a ransomware response plan as part of overall cybersecurity program activities.
* Schedule plan reviews and updates at least annually.
* Create a schedule of ransomware incident response activities during a calendar year, e.g., plan exercises, plan reviews, and training and awareness.
 | [ ]  |
| 12 | Appendixes  | Prepare and include relevant appendixes that support the incident response plan, such as forms, checklists and contact lists. | [ ]  |