**Ransomware Tabletop Exercise Template**

*By Paul Kirvan, FBCI, CISA*

Use the following template to help prepare a ransomware response plan exercise. Ideally, it should be part of an overall cybersecurity response exercise that includes responding to a variety of malware attacks, such as phishing, distributed denial of service, viruses, spam and ransomware. The template structure can be adapted to a variety of situations.

In the exercise, the participants have the list of activities in the column "Situation occurring." Exercise leaders have both "Situation occurring" and "What is the response?" columns, as they are looking at how the participants respond to the situations as they occur.

Both participants and leaders may mark down observations during the exercise and relay their findings after the exercise is complete.

|  | **Situation occurring** | **What is the response?** | **Observations** |
| --- | --- | --- | --- |
| 1. | Employees call into the help desk reporting they are unable to access certain systems |  |  |
| 2. | Alarms from firewalls and intrusion prevention system begin sounding |  |  |
| 3. |  | IT security staff examines alarms and makes initial assessment of a malware attack |  |
| 4. | Employees report they are unable to access files and databases, saying a code is needed to access them |  |  |
| 5. |  | IT staff examines code patterns captured by perimeter security systems |  |
| 6. | IT staff alerts senior IT management of a suspected ransomware attack |  |  |
| 7. |  | Senior IT staff alerts senior leadership of the attack and advises employees to log off their systems and back up their files as quickly as possible |  |
| 8. | IT staff examines various systems and determines that access to them has been blocked, notifies senior IT leadership |  |  |
| 9. |  | IT staff commences actions to isolate the malware for further examination |  |
| 10. | Employees and senior management are increasingly unable to access systems and files |  |  |
| 11. |  | Senior management instructs other leaders to identify any negative effects the attack may be causing, such as the inability to handle customer inquiries and place orders within their departments |  |
| 12. | Senior leaders inquire of their teams and determine that the attack is causing operational problems; share this information with IT |  |  |
| 13. |  | IT continues to assess the situation and examine the malware, which antimalware software has captured  |  |
| 14. | Senior leaders meet to determine if the company needs to shut down until the ransomware issue is fixed |  |  |
| 15. |  | Employees are instructed to leave the office and await further instructions on the cyber attack |  |
| 16. | Employees notify the help desk that they are unable to log in remotely  |  |  |
| 17. |  | IT determines the nature of the attack, secures a fix and uses the antimalware software to eliminate the malware |  |
| 18. | Employees and senior management still report they are unable to access systems and files |  |  |
| 19. |  | IT finds that the encryption used by the perpetrators is too difficult to decrypt; advises senior IT leaders |  |
| 20. | Senior management instructs IT to recover damaged system, files and other assets from backup copies  |  |  |
| 21. |  | IT commences system and file recovery using backed-up resources; cleans affected systems and network perimeter resources; reloads backed-up assets |  |
| 22. | Employees begin reporting they are able to access their systems and files |  |  |
| 23. |  | IT notifies senior IT leaders who notify senior company management  |  |
| 24. | IT sends notification to all employees that systems have been successfully recovered |  |  |
| 25. | Exercise ends |  |  |