*Terms of use: Only entities that are customers or partners of Lake Ridge Technologies, LLC are permitted to use this documentation template. This template may not be resold. By using this template, you are accepting the terms of use.*



Incident Response Exercises

Date of Exercise:

Participants:

# Scenario 1: Compromised User Account

Adam received a phishing email asking him to reset his Microsoft 365 password. The email appeared to come from Microsoft. Adam clicked the link and entered his old and “new” password on the form. Adam later noticed that his “new” password was not working so he contacted IT and informed them that he had just reset his password. IT checked the password reset logs and discovered that the password was not recently reset. Adam explained that he received an email where he clicked a link and “reset” his password. IT informed Adam that it was a phishing attack.

**Discussion Questions:**

As the incident response team, what actions would you take to contain and recover from this incident?

What actions can we take to prevent this incident from reoccurring?

# Scenario 2: Unauthorized Configuration Change

Bill is the system administrator at ACME. This morning the helpdesk received a few requests to share OneDrive files externally. Currently, OneDrive files can only be shared with whitelisted domains. To “resolve” the tickets, Bill adjusted the SharePoint/OneDrive file sharing settings to allow file sharing with anyone. Upon reviewing various logs and reports, Doug, ACME’s cybersecurity analyst noticed that files were being shared with unauthorized external users.

**Discussion Questions:**

As the incident response team, what actions would you take to contain and recover from this incident?

What actions can we take to prevent this incident from reoccurring?

# Scenario 3: Use of Unauthorized Cloud Storage

James is working with a customer and needs to share a large company document with them. He tried to share it with them using his company OneDrive, but the customer’s domain is not whitelisted in SharePoint/OneDrive. James decides to upload the company document to his personal Google Drive and shares it with the customer.

**Discussion Questions:**

As the incident response team, what actions would you take to contain and recover from this incident?

What actions can we take to prevent this incident from reoccurring?