Overview

Incident Response is a critical part of any Information Security Program to ensure that Private & Confidential information is protected. It is therefore important to not only have an Incident Response Plan in place, but to test the efficacy of the plan regularly. This document serves as demonstration for the 2025 Incident Response Plan testing for [CLIENT].

Methodology of Testing

The Incident Response Plan test took place encompasses 4 scenarios that simulate real-world security incidents that [CLIENT] may face. Scenarios are organized based on the affected localities and individuals within [CLIENT].

Each scenario is presented to key stakeholders for the documented Incident Response Plan and discussed in a "tabletop" manner. Escalating questions are utilized throughout the scenarios are also included to test the knowledge of the plan's procedures. Following the discussion, takeaways are documented to review and improve the plan as needed.

This test was performed on [DATE] 2025, with the following team members present:

- [NAME] - CFO
- [NAME] - CEO
- [NAME] - General Counsel
- [NAME] - Director, Communications & Marketing
- [NAME] - COO
- [NAME] - Head of Technology Operations and Security

- **Abacus Group GRC Team members:**
  - Mick Grayson – Manager of GRC
  - Khurem Ali – Senior GRC Analyst

Instructions for Testing

This test is intended to determine the current capability of [CLIENT] to detect, respond and remediate or mitigate security incidents based on [CLIENT]'s operations and current Incident Response Plan. The team will review the scenarios and respond to the questions to the best of their knowledge. Clarification questions may be asked to gain a more nuanced understanding of the scenario and determine the appropriate actions to be taken. If any team member is unsure of how to answer a question, that uncertainty will be used to improve the Incident Response Plan.

Analysis and Key Takeaways

Even though the exercise demonstrated that [CLIENT]'s Incident Response Plan is effective in identifying and responding to various security incidents, after reviewing the Table Top exercise, the following improvements have been suggested:

Topic	Rationale	Recommendation
No Data Classification / Labelling	Poor DLP controls can lead to accidental data exfiltration / mishandling	• Introduce & assign data classification & labelling through a solution such as Microsoft Purview • Educate users on data handling (including where files should be stored)
Update Acceptable Use Policies for Employees	Creating mechanisms to inform employees of what they should not be doing and establishing enforcement mechanisms	• Prohibit downloading files & sharing • Restrict SharePoint file sharing with customers only • Review sharing to public domains such as Gmail, etc • Review and confirm what apps/software are allowed on [CLIENT] devices • Review and confirm who has access to SharePoint files (both internally and externally) • Establish and enforce policies for AI (including CoPilot) usage

Topic	Rationale	Recommendation
Update Technical controls	Align technology with policy and provide enforcement mechanisms	• Block installation of WhatsApp on corporate devices (via device management software) • Implement an alert on password changes to Microsoft 365 (suspicious timing, locations, frequency, etc) in case compromised user does not contact helpdesk • Purchase Dynamics backup solution if necessary • Investigate if risk of having Dynamics in same tenant as other services is acceptable, else investigate solutions • Limit AI interaction within other services or implement DLP and access configurations on AI systems utilised for [CLIENT] operations
External Sharing	Even though external SharePoint sharing is allowed by design with external forwarding blocked, no controls can be enforced to prevent external users forwarding a downloaded copy of the data.	• Implement a DLP control mechanism to alert if externally shared data has been downloaded
Downtime	Even though X-X hours is within reason, for email communication which was a highlighted concern, this is too long	• Review disaster recovery tests of high availability systems managed by Abacus to validate expected downtime • Research and implement new strategies or solutions to have email services back up and running within a few hours, ideally within X hours of outage

In addition, while reviewing the Tabletop exercise, the following topics were not covered and are assumed to be missing overall. Therefore, it is suggested that the Incident Response Plan be verified to ensure the following are either covered or included going forward:

- Investigate if the threat actor:
    - Potentially manipulated data

    - Potentially installed malware onto the affected users' computers
        - If malware was, detected how it would be removed
    - Is an insider threat rather than a convenient compromised user
    - Can potentially to spread the ransomware through external SharePoint sharing to third parties
    - Identity & motives can be uncovered

- Confirm if internal processes:
    - Include patch & vulnerability management
    - Ensure antimalware and security solutions are consistently kept up to date

The recommendations above are made to improve the efficacy and efficiency of executing incident response plans but are not inherently critical to the execution of the plans. Any changes to plans or contracts should be discussed and approved internally with any key stakeholders within the Firm.

For further details on each scenario, please see the summarized notes below. These notes include specific missed topics per scenario, even if they were addressed at another stage, as consistency is key.

[CLIENT] Incident Scenarios

Compromised Staff Member

[CLIENT] has received a slew of phishing emails as of late attempting to get users to click a malicious link to a fake Microsoft 365 portal. A newer staff member clicked on the link and entered their credentials, including authorization to send an MFA token. The staff member is reporting that their credentials are no longer working, meanwhile Microsoft 365 audit logs are indicating that the most recent logins since the clicked phishing email have been utilizing a new form of MFA that the staff member does not recognize.

Topic	Action
Scenario risks & impact?	• Data breach / leakage outside of the organisation. • Lateral movement (compromising other staff members) • Access to information / systems that utilize SSO with the compromised credentials • Spreading compromise outside an organization / reputational risk from external parties receiving messages from the compromised account • Operational impacts (e.g., unable to perform job duties in a timely manner) • Wire fraud attempts using falsified identity
Processed / extracted data?	• Sensitive, finance, personal & customer data • Within Microsoft, SharePoint, OneDrive platform
Detection of compromise?	• Automated alerting tools • Processes (if password reset failed, it alludes to a serious issue) • User reports/tickets • Audit logs
Initial containment actions?	• Contact Abacus/IT MSP/Internal IT staff to alert of the situation • Lock, isolate & disable the affected user's account and any associated SSO • Revoke session • Reset credentials (passwords, MFA) • Anti money laundering controls are invoked if wire fraud attempts are made • Shut down necessary file servers
Remediation actions?	• Temporary revocation of access to potentially affected systems • Reset user credentials after containment • Perform forensic review and restore from valid backups • Force all devices to restart with approval to apply updates if necessary • Review all sharing domains & verify genuine access / share • Remove public access, ensuring customer access only
Investigation resources / capabilities?	• Logs (access/ audit logs on systems, security groups, SharePoint sites, any sent/forwarded emails) • RBAC tools • External consultants such as Abacus or pen test partners for specialised support

Topic	Action
Exfiltration options?	• Email • Download and share • External SharePoint sharing • Share to email domains such as Gmail etc • Poor DLP
Obligations / communications?	• Understand what communication needs to be sent • Senior leadership report • Potentially fellow colleagues if need arises to keep them informed • Clients / investors / third parties • GDPR, ICO assessment / notification within X hours • Contact Abacus & arrange for help
Cyber resiliency improvement?	• Implement internal communication monitoring mechanism upon compromise. • Introduce mechanism to detect mass email sending/sharing • End user awareness training • Identifying attempts to compromise accounts • Individual training • Alerting relevant parties • ID system logs / logs of other systems • Introduce adequate data classification & labelling in place • Stronger DLP solutions • Acceptable use policy needs updating with no sharing to personal email accounts • Perform regular security audits • Enhanced MFA • Lateral movement detection • Administrator privilege reviews • Information rights management (controlled sharing)
Current alerts / controls?	• Yellow caution banner for all external emails to warn for phishing • Alerts from a non-[CLIENT] device or non-approved device connects • SharePoint performs X backups, with annual tests and X RTO for full environment • Backups span a X period • Elevated controls to protect accounts from gaining administrative access • Phishing campaigns • Third Party risk assessment • Vulnerability management • Forwarding SharePoint sharing is blocked • Policy for employees to follow when discussing the incident (including social media guidelines) • Emails are kept infinitely with auto archive

Topic	Action
Missed topics	• Data Manipulation, falsified business data • Potential installation of malware onto the affected user's computer • Removal of Malware if detected • Anti-malware (Abacus – SentinelOne) • Notifications from users, IT MSP/Abacus • Review connected systems to determine if other non-SSO solutions have been affected • Email Security (Abacus - Mimecast) • SIEM (Abacus - Rapid7) • Insider threat rather than compromised user • Cyber insurance • Alerting law enforcement
Potential concerns	• Even though external SharePoint sharing is allowed by design, with external forwarding blocked, however no controls can be enforced to prevent external users forwarding a downloaded copy of the data. • If the compromised user doesn't call helpdesk, [CLIENT] remains in the dark, allowing the attacker more time.

System Outage – Disruption of Service

Whilst investigating the compromised staff member, more users are reporting being unable to access Microsoft 365, perhaps showcasing the threat actor is moving laterally within [CLIENT]'s network, impacting more users as time progresses. And thus will result in Microsoft 365 becoming temporarily inaccessible to more employees.

Topic	Action
Critical services affected?	• Microsoft 365 • Outlook • SharePoint • Financial Systems • Authentication services (Microsoft, SSO, MFA)
Maximum downtime?	• X – X Hours
Alternative solutions / procedures?	• Alternative Communication Channels • No other alternatives as primarily attempt to contain and minimise the service access as needed
Remediation actions?	• Utilise [CLIENT] Incident plan • Get critical systems back online with investigation in parallel • Disable MFA: Temporarily disable MFA to restore access. • Stop service front end to prevent lateral movement • Prioritise what teams/regions needed back online first • Reach out to third parties for help • Investigate logs
Potential lateral movement?	• Highly dependent on situation with potential lateral movement taking place
Investigation resources / capabilities?	• Logs (access/ audit logs on systems, security groups, SharePoint sites, any sent/forwarded emails) • RBAC tools • External consultants such as Abacus or pen test partners for specialised support
Obligations / communications?	• Inform employees about the outage, the steps being taken, and any actions they need to take • Financial requirements • Third parties (suppliers, fund admin) • Utilise Abacus as single helpdesk
Current alerts / controls?	• User alerts/tickets • Incident plan
Potential concerns	• Administrative burden to get critical people/services back online • Financial grace periods • If emails go down, potential difficulty to communicate

Ransomware

Upon getting their Microsoft 365 access repaired, the compromised staff member then reported that they were unable to access the files in their personal folder within OneDrive & SharePoint storage solutions, receiving an error about decrypting the files. In the same folder, a newly created document called “read me.txt” was discovered which contained instructions for paying a ransom in cryptocurrency to restore access to the files.

Topic	Action
Scenario risks & impact?	• Individual’s OneDrive • SharePoint • Data breach (employee data, HR, payroll, medical) • Business Operations • Data downloaded locally on attacker side • Uploading stolen data within dark web • Potential reputational damage
Access downtime?	• X – X Hours
Initial containment actions?	• Confirm if individual or system wide information • Take SharePoint tenant offline
Remediation actions?	• Prioritise backups & review any delta in backups • Perform forensic review and restore from valid backups • Consider paying ransom
Investigation resources?	• Business operations working document • Reach out to third parties for expertise to confirm scope extent • Conduct Forensic Analysis
Key indicators	• What data groups / localities have been cryptolocked
Exfiltration options	• Email • Download and share • External SharePoint sharing • Share to email domains such as Gmail etc • OneDrive
Backup options	• Perform forensic review and restore from valid backups • SharePoint performs X backups, with annual tests and X hour RTO for full environment • Back ups span a period of X years. • Emails are kept indefinitely with auto archive
Cyber resiliency improvement?	• Purchase Dynamics for Azure as a backup solution

Topic	Action
Obligations / communications?	• Inform employees • Cyber insurance • Law enforcement • Notification to ICO • Shareholders • Third parties • Utilise Abacus to assess the situation.
Current alerts / controls?	• Yellow caution banner for all external emails to warn for phishing • Only iPhone devices allowed • Alerts from a non [CLIENT] device or non-approved device connects • SharePoint performs X backups, with annual tests and X RTO for full environment • Backups span a X year period • Elevated controls to protect accounts from gaining administrative access • Phishing campaigns • Third Party risk assessment • Vulnerability management • Forwarding SharePoint sharing is blocked • Policy for employees to follow when discussing the incident (including social media guidelines) • Emails are kept infinitely with auto archive
Missed topics?	• Potentially spreading ransomware to external SharePoint shared third parties • Patch management • Ensure antimalware solutions are constantly up to date • Investigating threat actors identity & motives
Potential concerns	• Even though external SharePoint sharing is allowed by design, with external forwarding blocked, however no controls can be enforced to prevent external users forwarding a downloaded copy of the data. • If the compromised user doesn't call helpdesk, [CLIENT] remains in the dark, allowing the attacker more time. • Potential risk having dynamics in same tenant as everything else

Unauthorised Data Access

Whilst performing an investigation to better protect [CLIENT] in the future to ensure future Ransomware Attacks do not occur, you notice other pieces of information had been accessed by that same compromised individual showcasing unauthorised access to data has occurred. At the moment, you cannot verify if any data exfiltration could have taken place.

Topic	Action
Scenario risks & impact?	• Data breach / leakage outside of the organisation. • Lateral movement (compromising other staff members) • Access to information / systems that utilize SSO with the compromised credentials • Spreading compromise outside an organization / reputational risk from external parties receiving messages from the compromised account • Operational impacts (e.g., unable to perform job duties in a timely manner) • Wire fraud attempts using falsified identity
Initial containment actions?	• Contact Abacus/IT MSP/Internal IT staff to alert of the situation • Lock, isolate & disable the affected user's account and any associated SSO • Revoke session • Reset credentials (passwords, MFA) • Anti money laundering controls are invoked if wire fraud attempts are made • Shut down necessary file servers
Remediation actions?	• Temporary revocation of access to potentially affected systems • Reset user credentials after containment • Perform forensic review and restore from valid backups • Force all devices to restart with approval to apply updates if necessary • Review all sharing domains & verify genuine access / share • Remove public access, ensuring customer access only
Investigation resources?	• Logs (access/ audit logs on systems, security groups, SharePoint sites, any sent/forwarded emails) • RBAC tools • External consultants such as Abacus or pen test partners for specialised support • Understand impact • Investigate newly created / change shares / settings / access
Cyber resiliency improvement?	• Data classification labels • DLP alerts

Topic	Action
Current alerts / controls?	• Would have checked access rights on compromised user after first • Logs: Access and audit logs from affected systems. • RBAC • Access alerts • Mass file download / transfer alerts • Brute force alerts • Limited CoPilot licenses
Potential concerns	• AI & CoPilot