Incident Response Procedure – Best Practice Recommendations

Background

This Incident Response Procedure provides a framework for building an incident communication capability within a Supplier organization to communicate the appropriate information and details of a cyber incident in a timely manner to JPMorgan Chase & Co   ("JPMC") to meet JPMC's Minimum Control Requirements.

This Incident Response Procedure documents the steps and actions to be taken by the Supplier, and is meant to be used as a general guideline for incidents; however, specific responses and actions must be tailored to the incident, its size, scope and impact. It is not intended to replace or circumvent any of Supplier's existing procedures for the resolution of the actual incident. All of Supplier's other existing policies and procedures must be adhered to for the reporting, communication (regulatory, customer and media) and resolution of the specific incident(s).

Supplier Incident Communication Procedure

A Supplier must establish a formal incident communication procedure ("Response Procedure") to ensure its respective teams are familiar with their responsibilities in the event of an incident. A formal incident communication team made up of subject matter experts ("SMEs") and senior management with the authority & responsibility to communicate with JPMC is essential in timely dissemination of information.

An " incident" that would trigger the Response Procedure is any event which results in (y) unauthorized access to, disclosure or use of, or loss of integrity to (i) JPMC information; (ii) systems that store, process or transmit JPMC information; and/or (iii) systems that are otherwise used to provide JPMC services (including, but not limited to, source code repositories and software delivery systems); or (z) the unavailability of any service provided to JPMC that is a result of malicious activity, as well as any violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices

<u>Response Procedure Testing</u>

1. Have a documented Response Procedure runbook.
2. Test the runbook, through paper based table top exercises and through hands on keyboard simulations.
3. Get pre-approval (or have agreement on a fast approval process) from management and legal to share Indicators of Compromise (IOC) and Tactics, Techniques and Procedures (TTP) with law, government, partners and customers who request it.

Incident Response Procedure – Best Practice Recommendations

Incident Management Actions to be taken by Supplier

The following are the details JPMC will require during the initial communication:

Data Gathering:

1. Document/summarize the incident per table below

JPMC Communications:

1. Based upon immediately available information, Supplier communicates the incident to JPMC within the time frame set forth in the governing agreement with JPMC.
2. How to initially notify JPMC:
    a. Supplier can contact the JPMC Delivery Manager.
    b. Supplier can contact the JPMC Cyber Hotline 24x7 by phone 1877 576 7621; or
    c. Supplier can email Cyber.alert@jpmchase.com or JPMC.Supplier.Notifications@jpmchase.com.
3. Schedule conference call with JPMC Delivery Manager to explain the incident (details per table below) and determine next steps, which will be based on the nature and severity of the incident
    a. Conduct periodic conference calls to monitor the actions recommended by Supplier's respective teams or JPMC through completion.
    b. Ensure Supplier SMEs and senior management is made available to JPMC as needed.
    c. Provide periodic status update to JPMC Delivery Manager and to the JPMC Cyber Teams with which Supplier has been working.
4. Share relevant threat analysis (IP, IOCs, Forensic reports etc) with JPMC to ensure impact assessment.
5. Based on incident impact/severity, JPMC will determine additional actions to implement and any interim risk mitigation. For example, without limitation:
    a. Pull back/isolate data
    b. Shift temporarily to in-house/alternate provider
    c. Activate business continuity plan

Post Incident Response:

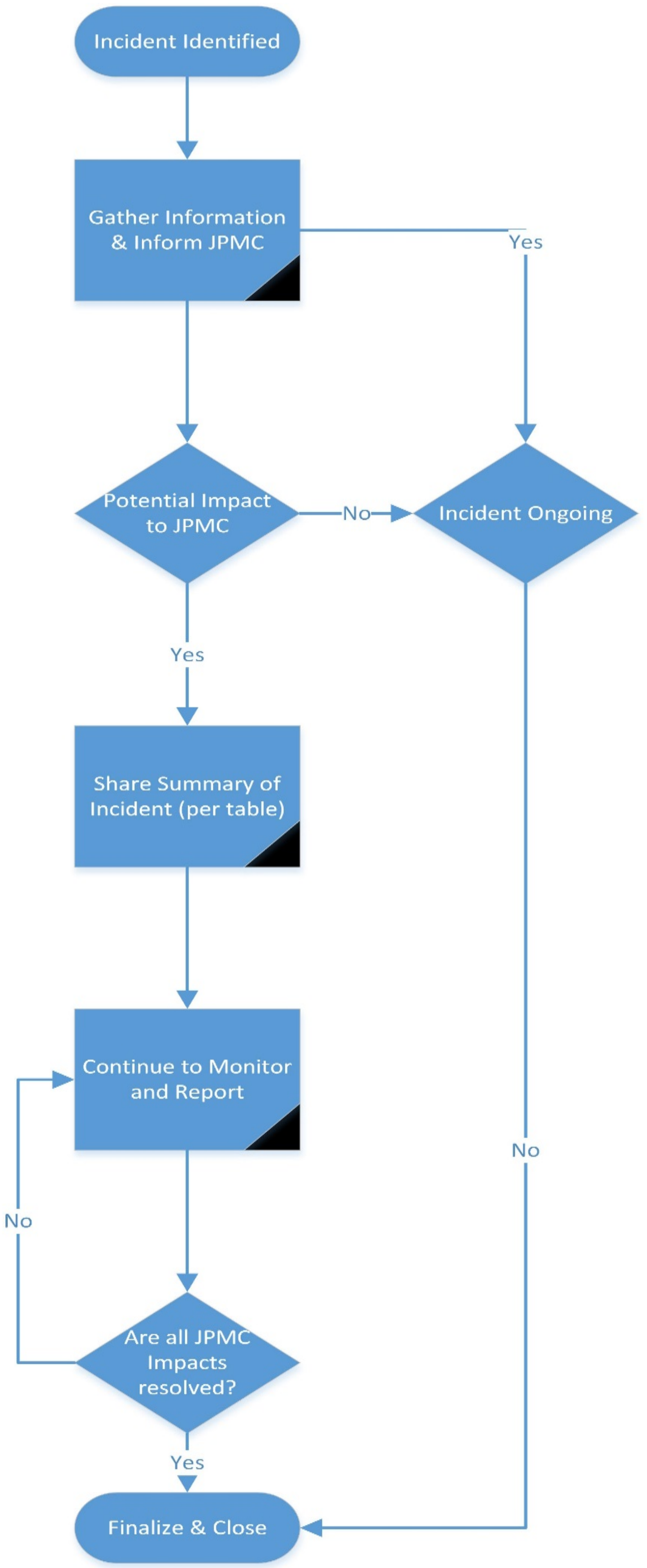
1. Discuss lessons learned and update controls where necessary.
2. Review and enhance Response Procedure runbook.
3. Store all incident response related documents for an adequate retention period as deemed appropriate period per legal and jurisdictional requirements.
4. Final report for distribution to JPMC stakeholders.

Incident Response Procedure – Best Practice Recommendations

Information Details JPMC will require:

Information	Description
Timing of Incident	What time did the incident occur?
Type of Incident	Virus, DDoS, ransomware, malicious attack , phishing, etc;
Nature of incident	A concise description of the identified incident and its potential JPMC impact (be as detailed as possible). In the event that data has been leaked or exfiltrated provide an indication of the extent of the data exposure and classification of data including JPMC impact.
Source of incident information	How was the breach discovered? For example, through notification from another party, from self-discovery, etc.
Investigation details	What actions have you taken as part of investigating the incident to confirm its potential scope and impact.
Remediation Activities	What actions are you taking (or have taken) to mitigate / remediate the incident? Have you engaged a 3rd party? Informed Legal authorities? Regulatory impact?
Impact Analysis	What is the JPMC impact analysis. For example, if there are any evidence in logs or the data that indicates unauthorized access to JPMC data.
Data Sharing	Are there audit logs? Indicators of Compromise (IOC)? Forensic reports?
Next Steps	What are your next steps? What's outstanding? Provide your timeline for full remediation and service restorations

Incident Response Procedure – Best Practice Recommendations



Incident Identified
Gather Information & Inform JPMC
Yes
Potential Impact to JPMC
No
Incident Ongoing
Yes
Share Summary of Incident (per table)
Continue to Monitor and Report
No
No
Are all JPMC Impacts resolved?
Yes
Finalize & Close