RakshaSutraX Incident Response

Phishing Playbook v1.0

Document Control

Title	Phishing Playbook
Version	1.0
Date Issued	0112/2024
Status	Draft
Document owner	RaptorX7
Creator name	RaptorX7
Creator organisation name	RakshaShutraX
Subject category	Cyber Incident Response Management
Access constraints	

Document Revision History

Version	Date	Author	Summary of changes
1.0	01/012/2024	RaptorX7	Generic Version Created from Public Sector Playbook

Contents

1. Introduction

1.1 Overview

In the event of a cyber incident, it is important that the organisation is able to respond, mobilise and execute an appropriate level of response to limit the impact on the brand, value, service delivery and the public, client and customer confidence. Although all cyber incidents are different in their nature and technologies used, it is possible to group common cyber incident types and methodologies together. This is in order to provide an appropriate and timely response depending on the cyber incident type. Incident specific playbooks provide incident managers and stakeholders with a consistent approach to follow when remediating a cyber incident.

References are made to both a Core IT CIRT and a CIRT within this document. This is in recognition the playbook will be used by organisations of different sizes. Some may initially manage an incident with a small response team within IT services, but, where there is a confirmed compromise, this may be escalated to an extended level CIRT comprising of members of the organisation outside the IT services who will deal with agreed categories of compromise. The Playbook as with the CIRP will require to be adjusted to reflect the organisational make up.

Playbooks describe the activities of those directly involved in managing specific cyber incidents. However, it is important to acknowledge the speed at which cyber incidents can escalate and become a significant business disruptor requiring both business continuity and consequence management considerations. Early consideration should be given to engaging Business Continuity, Resilience and Policy Area Leads in order that the wider issues can be effectively managed. Business Continuity and Resilience leads within the organisation must therefore be familiar with the Cyber Incident Response Plan (CIRP) and Playbooks and how they link to wider incident response arrangements.

1.2 Purpose

The purpose of the Cyber Incident Response: Phishing Playbook is to provide appropriate and timely response to a Phishing incident or attack. It is to define the activities that should be considered when detecting, analysing and remediating a Phishing incident or attack. The playbook also identifies the key stakeholders that may be required to undertake these specific activities.

1.3 Phishing Definition

Phishing is the act of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Spear Phishing is where an attacker uses information about employees and the company to make the Phishing campaign more persuasive and realistic.

1.4 Scope

This document has been designed for the sole use of the first responders such as the Service Desk team when responding to a cyber incident. It is not standalone and must be used alongside the Cyber Incident Response Plan (CIRP).

1.5 Review Cycle

This document is to be reviewed for continued relevancy by the Cyber Incident Response Team (CIRT) lead at least once every 12 months; following any major cyber incidents, a change of vendor, or the acquisition of new security services.

2. Preparation Phase

Preparation Phase		
Phase objectives	The preparation phase has the following objectives: • Prepare the organisation to respond to a cyber incident in a timely and effective manner; • Inform employees of their role in remediating a Phishing incident, including reporting mechanisms.	
Activity	**Description**	**Stakeholders**
Prepare to respond	Activities may include, but are not limited to:	
	Review and rehearse cyber incident response procedures including technical and business roles and responsibilities, escalation to major incident management where necessary.	• Head of Information Governance • CISO • Head of IT • Information Security Manager / ISO • Team Leader • Service Delivery Manager • Service Desk Analysts/Technicians • Legal Team • Communications Team • Police Area Lead • Resilience Lead • Business Continuity Lead
	Review recent cyber incidents and the outputs.	• Information Security Manager

	Review threat intelligence for threats to the organisation, brands and the sector, as well as common patterns and newly developing risks and vulnerabilities.	• Information Security Manager
	Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following: • CIRP; • <<Network Architecture Diagrams>>; (https://www.ibm.com/docs/en/power-virtual-server?topic=premises-network-architecture-diagrams) • <<Data Flow Diagrams>>:(https://www.sciencedirect.com/topics/computer-science/data-flow-diagram)	• Information Security Manager
	Identify and obtain the services of a 3rd party Cyber Forensic provider. Identify and secure the services of a 3rd party Cyber Responder Service	• Information Security Manager
	Define Threat and Risk Indicators and Alerting pattern within the organisation's security information and event management (SIEM) solution.	• Information Security Manager
Activity	**Description**	**Stakeholders**
Inform employees	Activities may include, but are not limited to:	
	Conduct regular awareness campaigns to highlight information security risks faced by employees, including: • Phishing attacks and malicious emails; • Ransomware; • Reporting a suspected cyber incident.	• Head of IT • Information Security Manager • Resilience Lead • Business Continuity Lead
	Ensure regular security training is mandated for those employees managing personal, confidential or high risk data and systems.	• Head of IT • Information Security Manager

		• HR • L&D Department • Resilience Lead • Business Continuity Lead

3. Detect

Detection Phase		
Phase objectives	The detection phase has the following objectives: • Complete initial investigation of the Phishing attack; • Report the Phishing attack formally to the correct team as a cyber incident.	
Activity	**Description**	**Stakeholders**
Detect and report the incident	Activities may include, but are not limited to:	
	Monitor detection channels, both automatic and manual, customer and staff channels and social media for indications of a data breach or compromise, these can include but are not limited to: • Spoofed emails; • Emails with links to external and unknown URLs; • Emails which are non-returnable or non-deliverable; • Notifications by internal users of suspicious emails; • Notifications by external users of customers of suspicious activity; • Notifications from Mimecast;	• Information Security Manager • Core IT CIRT • CIRT

	• Notifications from 3rd parties, law enforcement or ISP of suspicious activity.	
	Report the cyber incident via the Service Desk. If a ticket does not exist already, raise a ticket containing minimum information. To report an incident, follow the process defined in the CIRP.	• Information Security Manager • Core IT CIRT
	Consider whether data loss or data breach has occurred and if so refer to data breach playbook.	• Information Security Manager • Core IT CIRT
	Classify the cyber incident, based upon available information related to the Phishing attack and the incident types (**see CIRP**).	• Information Security Manager • Cote IT CIRT
	Check escalation procedures (**see CIRP**) and escalate as appropriate.	• Information Security Manager • Core IT CIRT • CIRT • Resilience Lead • Business Continuity Lead • Policy Area Lead
	Report the Cyber Incident in accordance with the organisation's CIRP. Consider the Intelligence value to other organisations and share on the CiSP	• Information Security Manager • Core IT CIRT • CIRT

	Where appropriate consider reporting requirements to Information Commissioner's Office (ICO), relevant regulator and or Competent Authority (NISD), National Cyber Centre (NCSC) and / or Police Scotland.	• Information Security Manager • Core IT CIRT • CIRT
ctivity	**Description**	**Stakeholders**
Initial investigation of the incident	Activities may include, but are not limited to:	
	Mobilise the Core IT CIRT to begin initial investigation of the cyber incident **(see staff contact details within Core CIRP).**	• Information Security Manager • Core IT CIRT • CIRT The following may also be included in the incident response team where appropriate for the incident: • Service Desk Analysts • Server Desk Technicians • Server Team • Mobile Device Team
	Identify spoofed email.	• Head of IT • Information Security Manager • Core IT CIRT

	Collate initial incident data including as a minimum the following: • Type of cyber incident; • How was the cyber incident reported; • How many users have received the Phishing email; • What has caused the cyber incident; • Location of detection(s), both physical and logical; • Number of affected assets across the organisation (initial), is this increasing?; • Additional reporting relating to affected assets, including AV logs, system event logs, and network monitoring logs; • Preliminary business impact; and • Any current action being undertaken.	• Head of IT • Information Security Manager • Core IT CIRT
	Secure artefacts, including copies of suspected malicious software and forensic copies of affected system(s) for future analysis.	• Information Security Manager • Core IT CIRT
	Research Threat Intelligence sources and consider Cyber Information Sharing Partnership (CiSP) submission to gain further intelligence and support mitigation by others.	• Information Security Manager • Core IT CIRT
	Review cyber incident categorisation to validate the cyber incident type as a Phishing attack and assess the incident priority, based upon the initial investigation. (**See CIRP for Incident Severity Matrix)**	• Information Security Manager • Core IT CIRT • CIRT • Resilience Lead • Business Continuity Lead
Activity	**Description**	**Stakeholders**
Incident reporting	Activities may include, but are not limited to:	
	Report the cyber incident in accordance with the organisation's CIRP.	• Information Security Manager

		• Core IT CIRT • CIRT
	Where appropriate consider reporting requirements to Information Commissioner's Office (ICO), relevant Regulator and/or Competent Authority (NISD), National Cyber Centre (NCSC) and / or Police Scotland	• Information Security Manager • CIRT
	Escalate in accordance with the CIRP.	• Information Security Manager • Core IT CIRT • CIRT Resilience Lead • Business Continuity Lead • Policy Area Lead
Activity	**Description**	**Stakeholders**
Establish the requirement for a full forensic investigation	Activities may include, but are not limited to:	
	Consider conducting a full forensic investigation, on the advice of legal counsel. All evidence handling should be done in line with the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence.	• Information Security Manager • Core IT CIRT • CIRT

4. Analyse

Analysis Phase		
Phase objectives	The analysis phase has the following key objectives: • Analyse the cyber incident to uncover the scope of the attack; • Identify and report potentially compromised data and the impact of such a compromise; • Establish the requirement for a full forensic investigation; • Develop a remediation plan based upon the scope and details of the cyber incident.	
Activity	**Description**	**Stakeholders**
Analyse the extent of the incident	Activities may include, but are not limited to:	
	Engage technical staff from resolver groups.	• Information Security Manager • Core IT CIRT • CIRT
	Identify and research whether; • Personal data is at risk (internal or external to the organisation); • Other SENSITIVE data is at risk, if so use the Data Loss Play-Book; • Public or personal safety is affected; • Services are affected and what they are; • You are able to control / record and measure critical systems; • There is any evidence of who is behind the attack; • There is internal knowledge behind the incident; • The act could be exploited by criminals.	• Information Security Manager • Core IT CIRT • CIRT • Resilience Lead • Business Continuity Lead • Police Area Lead
	Determine patch methods.	• Information Security Manager • Core IT CIRT

	Review affected infrastructure for indicators of compromise derived from the Phishing analysis to identify any additional compromised system(s).	• Information Security Manager • Core IT CIRT • CIRT
	Preserve all evidence to support attribution or anticipated legal action.	• Information Security Manager • Core IT CIRT • CIRT
	Examine threat intelligence feeds to determine if the Phishing attack is bespoke and targeted at specific individuals/senior stakeholders.	• Information Security Manager • Core IT CIRT • CIRT
	Verify all infected assets are in the process of being recalled and quarantined.	• Information Security Manager • Core IT CIRT • CIRT
Activity	**Description**	**Stakeholders**
Identify and report potentially compromised data	Activities may include, but are not limited to:	
	Identify any data or systems that have been affected.	• Information Security Manager • Core IT CIRT • CIRT
	Identify user credentials compromised or at risk.	• Information Security Manager • Core IT CIRT • CIRT
	Identify IT services being impacted.	• Information Security Manager • Core IT CIRT • CIRT
	Identify business impacts of the attack.	• Information Security Manager

		• Core IT CIRT • CIRT
	Identify how widespread the attack is across the organisation.	• Information Security Manager • Core IT CIRT • CIRT
	Identify the tools used to detect the attack.	• Information Security Manager • Core IT CIRT • CIRT
	Consider whether reporting suspected or confirmed unauthorised access to any personal data to the authority is appropriate at this stage.	• Information Security Manager • Core IT CIRT • CIRT
	Update senior stakeholders on any suspected or confirmed data breach including unauthorised access to: • Personal data; • Sensitive organisational data.	• Information Security Manager • Core IT CIRT • CIRT Resilience Lead • Business Continuity Lead • Policy Area Lead
	Report any suspected or confirmed data breach including any personal data breach to the appropriate parties.	• Information Security Manager • CIRT
Activity	**Description**	**Stakeholders**
Develop a remediation plan	Activities may include, but are not limited to:	
	Incorporate technical and business analysis to develop a prioritised remediation plan.	• Information Security Manager • Core IT CIRT • CIRT

	Implement a communications strategy in line with the remediation plan.	• Head of IT • Information Security Manager • CIRT • Communications Team • Resilience Lead • Business Continuity Lead • Policy Area Lead

5. Remediation – Contain, Eradicate and Recover

Remediation Phase		
Phase objectives	The remediation phase has the following objectives: • Contain the effects of the malware on the targeted systems; • Eradicate the malware from the network through agreed mitigation measures; • Recover affected systems and services back to a Business As Usual (BAU) state.	
Activity	**Description**	**Stakeholders**
Containment	Contain the technical mechanisms of the Phishing attack, including:	
	Identify systems being impacted or at risk of impact: • MS and Unix Servers; • Desktops; • Laptops; • Mobile devices; • VMs; • Network servers (e.g. DNS & IAM), switches and routers; • Support servers (Appliances, Hypervisor and Management Systems); • Database Servers.	• Information Security Manager • Core IT CIRT • CIRT • Resilience Lead • Business Continuity Lead • Policy Area Lead
	Reduce any further malicious activity by preventing the Phishing activity, quarantining affected systems and removing them from the network, or applying access controls to isolate from production networks.	• Information Security Manager • Core IT CIRT • CIRT
	Block access to any identified Remote Access Tools (RATs) to prevent communication with command and control servers, websites and exploited applications.	• Information Security Manager • Core IT CIRT • CIRT

	Identify compromised or at risk user credentials.	• Information Security Manager • Core IT CIRT • CIRT
	Identify malicious code on any systems linked to the fraudulent site.	• Information Security Manager • Core IT CIRT • CIRT
	Inform business data owner(s) and stakeholders of the progress of containment activities.	• Information Security Manager • Core IT CIRT • CIRT • Resilience Lead • Business Continuity Lead • Policy Area Lead
Activity	**Description**	**Stakeholders**
Eradication	Activities may include, but are not limited to:	
	Identify removal methods from the results of the attack.	• Information Security Manager • Core IT CIRT • CIRT
	Complete an automated or manual removal process to eradicate Phishing attack using appropriate tools.	• Information Security Manager • Core IT CIRT • CIRT
	Conduct a restoration of affected networked systems from a trusted back up.	• Information Security Manager • Core IT CIRT • CIRT

	Re-install any standalone systems from a clean OS back-up before updating with trusted data back-ups.	• Information Security Manager • Core IT CIRT • CIRT
	Change any compromised account details.	• Information Security Manager • Core IT CIRT • CIRT
	Confirm policy compliance across the estate.	• Information Security Manager • Core IT CIRT • CIRT
Activity	**Description**	**Stakeholders**
Recover to BAU	Activities may include, but are not limited to:	
	Recover systems based on business impact analysis and business criticality.	• Information Security Manager • Core IT CIRT • CIRT
	Complete vulnerability scanning of all systems, across the estate.	• Information Security Manager • Core IT CIRT • CIRT
	Re-set the credentials of all involved system(s) and users account details.	• Information Security Manager • Core IT CIRT • CIRT
	Reintegrate previously compromised systems.	• Information Security Manager • Core IT CIRT • CIRT
	Restore any corrupted or destroyed data.	• Information Security Manager • Core IT CIRT

		• CIRT
	Restore any suspended services.	• Information Security Manager • Core IT CIRT • CIRT
	Establish monitoring to detect further suspicious activity.	• Information Security Manager • Core IT CIRT • CIRT
	Co-ordinate the implementation of any necessary patches or vulnerability remediation activities.	• Information Security Manager • Core IT CIRT • CIRT

6. Post Incident

Post-Incident Activities Phase		
Phase objectives	The post-incident activities phase has the following objectives: • Complete an incident report including all incident details and activities; • Complete the lessons identified and problem management process; • Publish appropriate internal and external communications.	
Activity	**Description**	**Stakeholders**
Incident reporting	Draft a post-incident report that includes the following details as a minimum: • Details of the cyber incident identified and remediated across the network to include timings, type and location of incident as well as the effect on users; • Activities that were undertaken by relevant resolver groups, service providers and business stakeholders that enabled normal business operations to be resumed; • Recommendations where any aspects of people, process or technology could be improved across the organisation to help prevent a similar cyber incident from reoccurring, as part of a formalised lessons identified process.	• Senior Stakeholders • Head of Information Governance • Head of IT • CISO • Audit Committee • Information Security Manager • Resilience Lead • Business Continuity Lead • Policy Area Lead
Lessons Identified & Problem Management	Complete the formal lessons identified process to feedback into future preparation activities.	• Information Security Manager • CIRT
	Consider sharing lessons identified with the wider stakeholders where relevant.	• Information Security Manager • CIRT • Resilience Lead • Business Continuity Lead • Policy Area Lead • Legal Services

	Conduct root cause analysis to identify and remediate underlying vulnerabilities.	• Information Security Manager • Core IT CIRT • CIRT
Human Resource	Review staff welfare; working hours, over time, time off in lieu (TOIL) and expenses.	• Information Security Manager • HR • CIRT
Communications	Activities may include, but are not limited to:	
	Publish internal communications in line with the communications strategy to inform and educate employees on Phishing attacks and security awareness.	• Information Security Manager • Communications • HR • CIRT
	Publish external communications, if appropriate, in line with the communications strategy to provide advice to customers, engage with the market, and inform press of the cyber incident. These communications should provide key information of the cyber incident without leaving the organisation vulnerable or inciting further Phishing style attacks.	• Head of IT • Information Security Manager • Communications Team • CIRT

7. Annex A: Flow Diagram