RakshaSutraX Incident Response

Data Breach Playbook v1.0

Document Control

Title	Data Breach 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 4
   1.1. Overview 4
   1.2. Purpose 4
   1.3. Data Breach Definition 4
   1.4. Scope 4
   1.5. Review Cycle 5
2. Preparation Phase 6
3. Detect 7
4. Analyse 12
5. Remediation – Contain, Eradicate and Recover 16
6. Post Incident 20
7. Annex A: Flow Diagram 22

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 incidents types and methodologies together. This is in order to provide an appropriate and timely response depending on the cyber incidents type. Incident specific playbooks provide incident managers and stakeholders with a consistent approach to follow when remediating a cyber incidents.

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 comprised of members of the organisation outside IT services who will deal with agreed categories of compromise. The Playbook as with the Cyber Incident Response Plan (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: Data Breach Playbook is to define activities that should be considered when detecting, analysing and remediating a Data Breach incident. The playbook also identifies the key stakeholders that may be required to undertake these specific activities.

1.3. Data Breach Definition

A Data Breach is an incident, breach of security or wider privacy violation that leads to the accidental or unlawful destruction, unauthorised retention, misuse, breach, alteration, unauthorised disclosure of, or access to, data transmitted, stored or otherwise processed by the organisation, its employees, contractors or service providers.

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 incidents. It is not standalone and must be used alongside your 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 to respond to cyber incidents in a timely and effective manner; • Inform employees of their role in remediating a Data Breach incident including reporting mechanisms.	
Activity	**Description**	**Stakeholders**
Prepare to respond	Activities may include, but are not limited to:	
	Review and rehearse cyber incidents response procedures including technical and business roles and responsibilities, escalation to major incident management where necessary.	• Head of Information Governance • Head of IT • Information Security Manager • Team Leader • Service Delivery Manager • Service Desk Analysts/Technicians • Legal Team • Communications Team • 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>>; (insert Links) • <<Data Flow Diagrams>>.(insert Links)	• Information Security Manager
	Identify and obtain the services of a 3rd party Cyber Forensic provider.	• 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 cyber/information security risks faced by employees, including: • Legal and regulatory requirements around data security; • Phishing attacks and malicious emails; • Ransomware; • Reporting a suspected cyber incidents.	• 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: • Detect and report a breach or compromise of the confidentiality, integrity or availability of organisational/personal data; • Complete initial investigation of the Data Breach or compromise; • Report the Data Breach or compromise formally to the correct team as a cyber incidents.	
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: • Customers, employee or confidential data published online; • Clients or their customers being contacted by an unauthorised third party with access to personal or confidential information; • Targeted emails to clients or employees containing personal or confidential information; • Data breach prevention logs or alerts; • Lost or stolen devices containing confidential information;	• Information Security Manager • Core IT CIRT

	• Lost or stolen paperwork or hardcopies of data; • Other incidents that suggest data has been extracted outside of the network perimeter.	
	Report the cyber incidents 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 (Insert link to CIRP here).	• Information Security Manager • Core IT CIRT
	Classify the cyber incidents, based upon available information related to the Data Breach and the incident types (see CIRP).	• Information Security Manager# • Core IT CIRT
	Report the Cyber incidents 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
	Where appropriate consider reporting requirements to Information Commissioner's Office (ICO), relevant regulator and or Competent Authority (NISD), National Cyber Security Centre (NCSC) and / or Police Scotland	• Information Security Manager • CIRT • Resilience Lead • Business Continuity Lead • Policy Area Lead
Activity	**Description**	**Stakeholders**
Initial investigation of the incident	Activities may include, but are not limited to:	
	Mobilise the CIRT to begin initial investigation of the cyber incidents (see staff contact details within CIRP).	• Information Security Manager • Core IT 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 likelihood of employee involvement and notify HR (e.g. insider threat).	• Information Security Manager • Core IT CIRT • HR
	Collate initial incident data including as a minimum for the following; • How was the cyber incidents reported; • What has caused the cyber incidents (i.e. lost laptop, suspected hacker, malware. Etc.); • Location of data, both physical and logical; • Quantity of data i.e. number of accounts, unique numbers, client names; • Is financial data included? i.e. credit card numbers, pins, expiry dates, etc.? • Is personal data included? i.e. names, address, postcodes, email address, etc.? • What is the format of the data i.e. redacted, encrypted, layout, length, etc.? • Was there any encryption around the data and if so how was this provided? • Preliminary business impact assessment; and • Any current action being undertaken.	• Information Security Manager • Core IT CIRT
	Secure artefacts, including copies of the data, via secure download and screenshot.	• Information Security Manager • Core IT CIRT
	Review critical systems and assess for any indicators of similar data sets being compromised.	• Information Security Manager • Core IT CIRT

	Identify possible sources or owners of the data.	• Information Security Manager • Core IT CIRT
	Preliminary review of data involved to determine if personal data has been compromised.	• Information Security Manager • Core IT CIRT
	Research Threat Intelligence sources and consider Cyber Security Information Sharing Partnership (CiSP) submission to gain further intelligence and support mitigation by others.	• Information Security Manager • Core IT CIRT
	Review cyber incidents categorisation to validate the cyber incidents type as a Data Breach incident and assess the incident priority, based upon the initial investigation. (See CIRP for Incident Severity Matrix)	• Information Security Manager • Core IT CIRT
Activity	**Description**	**Stakeholders**
Incident reporting	Activities may include, but are not limited to:	
	Report the cyber incidents in accordance with the organisation's CIRP.	• Information Security Manager • Core IT CIRT • CIRT
	Immediately report Data Breaches that have occurred to the relevant Data Protection Officer. Consider whether reporting suspected or confirmed unauthorised access to any personal data to the authority is appropriate at this stage.	• Head of IT • Information Security Manager • CIRT • Head of Information Governance • Data Protection Officer
	Where appropriate consider reporting requirements to Information Commissioner's Office (ICO), relevant Regulator and or Competent Authority (NISD), National Cyber Security Centre (NCSC) and / or Police Scotland	• Head of IT • Information Security Manager • CIRT

		• Head of Information Governance • Data Protection Officer
	Report the Cyber incidents 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 Security Centre (NCSC), Police Scotland and / or Police Scotland	• Information Security Manager • Core IT CIRT • CIRT
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

4. Analyse

Analysis Phase		
Phase objectives	The analysis phase has the following key objectives: • Analyse the cyber incidents 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 incidents.	
Activity	**Description**	**Stakeholders**
Analyse the extent of the incident	Activities may include, but are not limited to:	
	Confirm any data involved is: • Legitimate; • Current; • Originating from the organisation; • Connected to the organisation or its Clients or their Customers.	• Head of IT • Information Security Manager • Head of Information Governance • Core IT CIRT
	Conduct a detailed technical investigation of the cyber incidents which may include, but is not limited to: • Analyse any suspicious network traffic; • Review security and access logs, vulnerability scans and any automated tool outputs; • Analyse any suspicious activity, files or identified malware samples; • Review AV logs or events, without jeopardising future forensic activities; • Correlate any recent security events, or indicators of compromise, with suspicious activity seen on the network;	• Information Security Manager • Core IT CIRT

	• Identify the source of the data compromise; • Identify the specific data set which was compromised as well as how it was compromised.	
	Determine the attack methodology and cyber incidents timeline.	• Information Security Manager • Core IT CIRT
	Analyse the data types and quantities to determine if there has been a privacy breach (i.e. involving personal data).	• Information Security Manager • Core IT CIRT
	Analyse the data types and quantities to determine if there has been a breach of financial data (e.g. organisational financial reports, customer or employee credit card details, bank details etc.).	• Information Security Manager • Core IT CIRT
	Analyse the data types and quantities to determine if the data is only found in the organisation's environments, or shared with third party systems.	• Information Security Manager • Core IT CIRT
	Review the data type and quantity compromised for any compliance regulations that have been breached.	• Information Security Manager • Core IT CIRT • CIRT
Activity	**Description**	**Stakeholders**
Identify and report potentially compromised data	Activities may include, but are not limited to:	
	Engage data owners and senior stakeholders to understand the business impact of the compromised data.	• Information Security Manager • Core IT CIRT • CIRT
	Report the cyber incidents in accordance with the CIRP, as required.	• Information Security Manager • Core IT CIRT

		• CIRT
	Establish the likelihood that confidentiality, integrity or availability has been compromised.	• 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 the senior stakeholders (see CIRP) of any suspected or confirmed Data Breach including the unauthorised access to any personal data.	• Information Security Manager • Core IT CIRT • CIRT
	In line with the GDPR (Article 33) the ICO must be informed within 72 hours of the organisation becoming aware of an incident resulting in a “risk to the rights and freedoms of those involved”. 1. **Reporting Data Breaches in India:** For Indian organizations, breaches related to personal or sensitive data need to be reported to the **Indian Computer Emergency Response Team (CERT-In)**. Here is the guidance for reporting: 2. **Visit the CERT-In Reporting Page:** ○ Access the CERT-In Reporting Page.to submit a report. (https://www.cert-in.org.in/s2cMainServlet?pageid=PUBWEL01) 3. **Follow CERT-In's Reporting Guidelines:** ○ Provide information such as the type of breach, affected data, and the organization's response. 4. **Notification and Compliance:**	• Information Security Manager • CIRT • Data Protection Officer

	○ Ensure that the breach is reported as per Indian laws, including the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**. .	
	Where a decision to notify the ICO has been made the following must be included as a minimum: • Describe the nature of the personal Data Breach including where possible, the categories and approximate number of data subjects and personal data records concerned. • Communicate the name and contact details of the contact point where more information can be obtained. • Describe the likely consequences of the personal Data Breach. Describe the measures taken or proposed to be taken to address the personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Consider other Reporting requirements such as Reporting as a crime to Police Scotland or to Regulators or Competent Authorities where relevant	• Information Security Manager • CIRT • Data Protection Officer
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.	• Information Security Manager • Core IT CIRT • CIRT

5.Remediation – Contain, Eradicate and Recover

Remediation Phase		
Phase objectives	The remediation phase has the following objectives: • Contain the technical mechanism of the Data Breach; • Eradicate the technical mechanism of the Data Breach; • Recover affected systems and services back to a Business As Usual (BAU) state.	
Activity	**Description**	**Stakeholders**
Containment	Contain the technical mechanisms of the Data Breach, including:	
	Isolate all affected systems or accounts from the infrastructure through removal from the network or application of strict access controls, to prevent further data exfiltration.	• Information Security Manager • Core IT CIRT
	Implement rules to block detected suspicious traffic leaving the network.	• Information Security Manager • Core IT CIRT
	Secure copies of infected systems and malware for further investigation, if not already completed.	• Information Security Manager • Core IT CIRT
	Reverse engineer malware to identify the indicators of compromise that will assist with eradication phase.	• Information Security Manager • Core IT CIRT
	Safeguard critical assets to prevent further harm or theft of data.	• Information Security Manager • Core IT CIRT

	Remotely erase any lost or stolen assets where possible.	• Information Security Manager • Core IT CIRT
	Reset passwords of legitimate user accounts and reduce permissions where possible.	• Information Security Manager • Core IT CIRT
	Isolate unauthorised user accounts and analyse any remove data stored.	• Information Security Manager • Core IT CIRT
	Contain the business effects of the cyber incidents:	
	Implement the notification strategy including any internal or external notifications, the notification of employees, third parties, service providers and customers.	• Information Security Manager • Core IT CIRT • CIRT
	Support the development of external communications by providing accurate, simple lines to take, in line with technical remediation activities.	• Information Security Manager • CIRT • Comms
	Engage the Data Protection Authority in the country where the compromise took place, if appropriate.	• Information Security Manager • CIRT • Data Protection Officer • Legal Services
Activity	**Description**	**Stakeholders**
Eradication	Activities may include, but are not limited to:	
	Remove any malware identified during the analysis phase using appropriate tools.	• Information Security Manager • Core IT CIRT

	Remove any identified artefacts used to facilitate the breach, such as scripts, code and binaries.	• Information Security Manager • Core IT CIRT
	Disable system and user accounts that have been used as a platform to conduct the attack.	• Information Security Manager • Core IT CIRT
	Identify common removal methods from trusted sources (AV providers).	• Information Security Manager • Core IT CIRT
	Complete an automated or manual removal process of the malware using appropriate tools.	• Information Security Manager • Core IT CIRT
	Conduct a restoration of affected networked systems from a trusted back up.	• Information Security Manager • Core IT 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
	Change any compromised account details.	• Information Security Manager • Core IT CIRT
	Confirm policy compliance across the estate.	• Information Security Manager • Core IT CIRT • CIRT
Activity	**Description**	**Stakeholders**
	Activities may include, but are not limited to:	

Recover to BAU	Recover systems based on business impact analysis and business criticality.	• Information Security Manager • Core IT CIRT • CIRT
	Complete AV and advanced malware scanning of all systems, across the estate.	• Information Security Manager • Core IT CIRT
	Re-set the credentials of all involved system(s) and users account details.	• Information Security Manager • Core IT CIRT
	Reintegrate previously compromised systems.	• Information Security Manager • Core IT CIRT
	Restore any corrupted or destroyed data.	• Information Security Manager • Core IT CIRT
	Restore any suspended services.	• Information Security Manager • Core IT CIRT
	Establish monitoring to detect further suspicious activity.	• Information Security Manager • CIRT • SIEM Provider
	Co-ordinate the implementation of any necessary patches or vulnerability remediation activities.	• Information Security Manager • Core IT 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 cause, impact and actions taken to mitigate the cyber incidents, and including, 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 incidents from reoccurring, as part of a formalised lessons identified process.	• Senior Stakeholders • Head of Information Governance • Head of IT • Audit Committee • Information Security Manager • Resilience Lead • Business Continuity Lead • Police Lead
Lessons Identified & Problem Management	Complete the formal lessons identified process to feedback into future preparation activities.	• Information Security Manager • CIRT
	Conduct root cause analysis to identify and remediate underlying vulnerabilities.	• Information Security Manager • Core IT CIRT • CIRT
	Consider sharing lessons identified with external stakeholders where relevant	• Information Security Manager

		• CIRT • Resilience Lead • Business Continuity Lead • Policy Lead
Human Resources	Review staff welfare; working hours, over time, time off in lieu (TOIL) and expenses.	• Information Security Manager • HR
Communications	Activities may include, but are not limited to:	
	Publish internal communications to inform and educate employees on Data Breach attacks and security awareness.	• Information Security Manager • CIRT • Communications
	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 incidents. These communications should provide key information of the cyber incidents without leaving the organisation vulnerable or inciting further Data Breach attacks.	• Head of IT • Information Security Manager • Communications Team • Resilience Lead • Business Continuity Lead • Policy Lead

7.Annex A: Flow Diagram