



RakshaSutraX Incident Response

Ransomware Playbook v1.0





Document Control

Title	Ransomware 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.	Ransomware Definition	4
1.4.	Scope	5
1.5.	Review Cycle	5
2.	Preparation Phase	6
3.	Detect	8
4.	Analyse	12
5.	Remediation – Contain, Eradicate and Recover	15
6.	Post Incident	19
7.	Annex A: Flow Diagram	21



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 of the different size and capabilities of organisations. 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 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 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 CIRP and Playbooks and how they link to wider Incident response and Exercising Playbooks and arrangements.

1.2. Purpose

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



1.3. Ransomware Definition

Ransomware is a type of malicious software in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access is returned to the victim. The motive for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions on how to recover from the attack.

1.4. Scope

This document has been designed for the 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 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: <ul style="list-style-type: none">• Prepare to respond to cyber incident in a timely and effective manner;• Inform employees of their role in remediating a Ransomware 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:- <ul style="list-style-type: none">• technical and business roles and responsibilities• escalation to major incident management, where necessary	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none"> Information Security Manager
	Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following: <ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> Information Security Manager
	Identify and obtain the services of a 3 rd party Cyber Forensic provider.	<ul style="list-style-type: none"> Information Security Manager
	Define Threat and Risk Indicators and Alerting pattern within the organisation's security information and event management (SIEM) solution.	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Phishing attacks and malicious emails; Ransomware; Reporting a suspected cyber incident. 	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Detect and report a breach or compromise of the confidentiality, integrity or availability of organisational data;• Complete initial investigation of the Ransomware;• Report the Ransomware attack or compromise data 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:	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT



	<ul style="list-style-type: none"> Automated AV alerts Detection from email filters Unusual activity on end-point devices, servers or phones Reports from end-users 	
	<p>Report the cyber incident via the Service Desk. If a ticket does not exist already, raise a ticket containing minimum information.</p> <p>To report an incident, follow the process defined in the CIRP.</p>	<ul style="list-style-type: none"> Information Security Manager Core IT CIRT
	<p>Consider whether data loss or data breach has occurred and if so <u>refer to data breach playbook</u>.</p>	<ul style="list-style-type: none"> Information Security Manager Information Governance Team
	<p>Classify the cyber incident, based upon available information related to the data loss and the incident types (see CIRP).</p>	<ul style="list-style-type: none"> Information Security Manager Core IT CIRT
	<p>Report the cyber incident in accordance with the organisation's CIRP.</p> <p>Consider the Intelligence value to other organisations and share on the CiSP</p>	<ul style="list-style-type: none"> Information Security Manager Core IT CIRT CIRT
	<p>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</p>	<ul style="list-style-type: none"> Information Security Manager Core IT CIRT CIRT
Activity	Description	Stakeholders
	Activities may include, but are not limited to:	



Initial investigation of the incident	Mobilise the CIRT to begin initial investigation of the cyber incident (see staff contact details within CIRP).	<ul style="list-style-type: none"> • Information Security Manager • Core IT CIRT <p>The following may also be included in the incident response team where appropriate for the incident:</p> <ul style="list-style-type: none"> • Service Desk Analysts • Server Desk Technicians • Server Team • Mobile Device Team
	Identify likelihood of widespread Ransomware infection.	<ul style="list-style-type: none"> • Head of IT • Information Security Manager • Core IT CIRT • CIRT
	Collate initial incident data including as a minimum for following; <ul style="list-style-type: none"> • Type of cyber incident; • How was the cyber incident reported; • Where are Ransomware messages appearing; • Identify the attack email; • 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. 	<ul style="list-style-type: none"> • Head of IT • Information Security Manager • Core IT CIRT • CIRT
	Secure artefacts, including copies of suspected malicious software and forensic copies of affected system(s) for future analysis.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> Information Security Manager Core IT CIRT
	Review cyber incident categorisation to validate the cyber incident type as a Ransomware attack and assess the incident priority, based upon the initial investigation. (See CIRP for Incident Severity Matrix)	<ul style="list-style-type: none"> Information Security Manager Core IT CIRT
Activity	Description	Stakeholders
Incident reporting	Activities may include, but are not limited to:	
	Report the cyber incident in accordance with the organisation's CIRP. Specifically Consider the Intelligence value to other organisations and share on the CiSP	<ul style="list-style-type: none"> Information Security Manager CIRT
	Consider whether the Incident meets the Scottish Public Sector cyber Incident Central Notification and Co-ordination Policy as contained within the CIRP.	<ul style="list-style-type: none"> Information Security Manager CIRT CIRT Resilience Lead Business Continuity Lead
	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	<ul style="list-style-type: none"> Information Security Manager Core IT CIRT CIRT
Activity	Description	Stakeholders

Commented [A1]: Public Sector Specific, consider removal



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.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT• CIRT



4. Analyse

Analysis Phase		
Phase objectives	<p>The analysis phase has the following key objectives:</p> <ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Service Desk Technicians• Core IT CIRT
	Classify the ransomware by submission to multiple AV vendors and determine the family it belongs to.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Scope the attack. <ul style="list-style-type: none">• Where are ransom messages appearing?• Are there any infected network drives? Which?• Identify the attack email or ingress point and the extent of travel.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Reverse-engineer the Ransomware in a secure environment to understand its mechanisms, and the functionality it implements.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT• External Security Partner



		<ul style="list-style-type: none"> • NCSC • Police Scotland
	Execute the Ransomware in a secure environment or sandbox, segregated from the business network, to determine its behaviour on a test system, including created files, launched services, modified registry keys and network communications.	<ul style="list-style-type: none"> • Information Security Manager • Core IT CIRT • External Security Partner • NCSC • Police Scotland
	Review affected infrastructure for indicators of compromise derived from the malware analysis to identify any additional compromised system(s).	<ul style="list-style-type: none"> • Information Security Manager • Core IT CIRT
	Preserve all evidence to support attribution or anticipated legal action.	<ul style="list-style-type: none"> • Information Security Manager • Core IT CIRT
	Examine threat intelligence feeds to determine if the ransomware attack is bespoke and targeted at specific accounts, infrastructure or systems.	<ul style="list-style-type: none"> • Information Security Manager • Core IT CIRT
	Verify all infected assets are in the process of being recalled and quarantined.	<ul style="list-style-type: none"> • 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 impacted by the ransomware attack, including data-in-transit.	<ul style="list-style-type: none"> • Information Security Manager • Core IT CIRT • CIRT



	Engage data owners and the business to understand the business impact of the compromised data.	<ul style="list-style-type: none"> • Information Security Manager • CIRT • Head of IT
	Report the Cyber incident to the organisation's senior stakeholders, as required.	<ul style="list-style-type: none"> • Information Security Manager • CIRT
	Establish the likelihood that identified data's confidentiality, integrity or availability was compromised.	<ul style="list-style-type: none"> • Information Security Manager • Core IT CIRT • CIRT
	<p>Consider whether reporting suspected or confirmed unauthorised access to any personal data to the Information Commissioner's Office (ICO) is appropriate at this stage.</p> <p>Consider reporting to incident to Police Scotland</p> <p>Consider reporting requirements to relevant regulator or Competent Authority if applicable</p>	<ul style="list-style-type: none"> • Information Security Manager • CIRT • Data Protection Officer • Legal Services
	Update the senior stakeholders of any suspected or confirmed data breach including the unauthorised access to personal or sensitive organisational data.	<ul style="list-style-type: none"> • Information Security Manager • CIRT • Data Protection Officer
	CIRT to immediately report any suspected or confirmed data breach including any personal/ data breach to the appropriate parties (refer to data loss/breach playbook).	<ul style="list-style-type: none"> • Information Security Manager • CIRT • Data Protection Officer • Legal Services`
	Consider Intelligence Sharing value on CiSP	<ul style="list-style-type: none"> • Information Security Manager • Resilience Lead



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.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT• CIRT
	Implement a communications strategy in line with the remediation plan.	<ul style="list-style-type: none">• Head of IT• Information Security Manager• CIRT• Communications Team• Resilience Lead• Business Continuity Lead



5. Remediation – Contain, Eradicate and Recover

Remediation Phase		
Phase objectives	<p>The remediation phase has the following objectives:</p> <ul style="list-style-type: none">• Contain the effects of the ransomware on the targeted systems;• Eradicate the ransomware 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 ransomware attack, including:	
	Reduce any further malicious activity by quarantining affected systems and removing them from the network, where possible, or applying access controls to isolate from production networks.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT• CIRT
	Develop protection measures derived from the results of malicious code analysis to protect infrastructure from the malicious code and other ransomware that may attempt to infect using the same mechanism.	<ul style="list-style-type: none">• Information Security Manager• CIRT
	Define scope by searching for: <ul style="list-style-type: none">• The SHA-1 process name;• The executable file name;• The URL or IP address of similar connections on the network.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	In the case of an email attack:	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT



Remediation Phase		
	<ul style="list-style-type: none">• Block the sender and the message by marking it as spam;• Block the IP address identified in the email header. <p>In the case of a website compromise:</p> <ul style="list-style-type: none">• Block the website at the network perimeter;• Sinkhole the domain on internal DNS servers;• Block the site IP address on the network firewall;• Ensure all web browsers used within DANB have the latest patches;• Encourage users to switch to newer browsers.	
	Block access to any identified Remote Access Tools (RATs) to prevent communication with command and control servers, websites and exploited applications.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Suspend the login credentials of suspected compromised accounts.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Secure copies of the malicious code, affected systems and any identified artefacts for further investigation (engaging with forensic support if forensic copies are required).	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Inform business data owner(s) and stakeholders of the progress of containment activities.	<ul style="list-style-type: none">• Information Security Manager
	Remind users to move the attack email to the 'Junk' folder.	<ul style="list-style-type: none">• Information Security Manager



Remediation Phase		
Activity	Description	Stakeholders
Eradication	Activities may include, but are not limited to:	
	Identify removal methods from the results of the malicious code analysis and trusted sources (AV providers).	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Complete an automated or manual removal process to eradicate ransomware or compromised executables using appropriate tools.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Conduct a restoration of affected networked systems from a trusted back up.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Re-install any standalone systems from a clean OS back-up before updating with trusted data back-ups.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Change any compromised account details.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Continue to monitor for signatures and other indicators of compromise to prevent the ransomware attack from re-emerging.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Confirm policy compliance across the estate.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT• CIRT



Remediation Phase		
Activity	Description	Stakeholders
Recover to BAU	Activities may include, but are not limited to:	
	Recover systems based on business impact analysis and business criticality.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT• CIRT
	Complete Ransomware scanning of all systems, across the estate.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Re-image systems.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Re-set the credentials of all involved system(s) and users account details.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Reintegrate previously compromised systems.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Restore any corrupted or destroyed data.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Restore any suspended services.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT
	Establish monitoring to detect further suspicious activity.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT



Remediation Phase		
	Co-ordinate the implementation of any necessary patches or vulnerability remediation activities.	<ul style="list-style-type: none">• Information Security Manager• Core IT CIRT



6. Post Incident

Post-Incident Activities Phase		
Phase objectives	The post-incident activities phase has the following objectives: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Details of the cause, impact and actions taken to mitigate the cyber incident, and including timings, type and location of incident as well as the effect on users;• Activities undertaken by relevant resolver groups, service providers and business stakeholders that enabled normal business operations to resume;• 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.	<ul style="list-style-type: none">• Senior Stakeholders• Head of Information Governance• Head of IT• Audit Committee• Information Security Manager• Resilience Lead• Business Continuity Lead
Lessons Identified & Problem Management	Complete the formal lessons identified process to feedback into future preparation activities.	<ul style="list-style-type: none">• Information Security Manager• CIRT



Post-Incident Activities Phase		
	Consider sharing lessons identified with the wider Indian Public Sector.	<ul style="list-style-type: none"> Information Security Manager CIRT Resilience Lead Business Continuity Lead
	Conduct root cause analysis to identify and remediate underlying vulnerabilities.	<ul style="list-style-type: none"> Information Security Manager Core IT CIRT CIRT
Human Resources	Review staff welfare; working hours, over time, time off in lieu (TOIL) and expenses.	<ul style="list-style-type: none"> Information Security Manager HR
Communications	Activities may include, but are not limited to:	
	Publish internal communications to inform and educate employees on ransomware attacks and security awareness.	<ul style="list-style-type: none"> Information Security Manager CIRT Communications
	<p>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.</p> <p>These communications should provide key information of the cyber incident without leaving the organisation vulnerable or inciting further ransomware attacks.</p>	<ul style="list-style-type: none"> Head of IT Information Security Manager Communications Team



7. Annex A: Flow Diagram

