National Cyber Security Centre | PART OF THE GCSB

# Rolls & Responders

## Facilitator Manual



**Version 1.0**

This page is intentionally left blank.

# Contents





National Cyber Security Centre | *PART OF THE GCSB*

# Discussion Prompts

This checklist shows factors and tasks that teams should consider when standing up their response. You can use it to prompt teams and ask questions they might not have considered.

| At all times | |
|---|---|
| | Document all actions |
| | Change management |
| | Preserve, secure, and protect evidence |
| | Data backup requirements |
| | Legal reporting requirements |

| Detection and triage | |
|---|---|
| | Determine validity of detection/report |
| | Determine resource requirements and affected parties |
| | Risk assessment: life and health |
| | Risk assessment: data (PII, sensitive information, etc) |
| | Assign incident lead |
| | Assess severity |
| | Assess indirectly exposed data or systems |

| Containment | |
|---|---|
| | Contain the threat |
| | Determine potential spread |
| | Assess actual spread |

| General | |
|---|---|
| | Who are your service providers? |
| | What is your organisations stance on paying a ransom? |
| | Have you established your roles and responsibilities? |

| Eradication | |
|---|---|
| | Detect root cause |
| | Remediate / Eliminate root cause |
| | Prevent reoccurrence |

| Termination | |
|---|---|
| | Notify senior management (Post-mortem) |
| | Investigation report |
| | Contact external agencies |
| | Improve future monitoring, procedures, tools, and policies |

| Communications | |
|---|---|
| | Create an incident reporting channel |
| | Communications plans (internal & external) |
| | Notify other teams (Legal, HR, Trust & Safety, Privacy, Security, Comms, Management, Executives) |
| | Contact external stakeholders (customers, vendors, etc.) |
| | Contact external agencies (Police, NCSC, etc.) |
| | Determine what the triggers for proactive communications are |

# Quick Play Scenarios

These quick play scenarios have been designed for a Facilitator to pick up and run with minimal additional planning.

| Difficulty | Scenario Description |
|---|---|
| Easy | **DDoS Attack**<br>A DDoS attack targets your organisation. The DDoS attack is from a paid stressor service hired by a group of criminals intending to extort your organisation for Bitcoin. Customers and senior stakeholders are becoming irritated. |
| Medium | **Ransomware**<br>Ransomware attack by hired security testers. Admin laptop compromised, user reported that machine boots into ransomware screen. Low-profile USB drive in one of the ports. |
| Hard | **Cloud Infrastructure Compromise**<br>The organisation has had their cloud infrastructure compromised by an attacker, leading to exfiltration of PII and unwanted media attention. |

**Distributed Denial of Service (DDos)** Difficulty level:

**Scenario Code**: 4452 (Extra Injects: 11, 8, 6)

**Description:** A DDoS attack targets your organisation. The DDoS attack is from a paid stressor service hired by a group of criminals intending to extort your organisation for Bitcoin. Customers and senior stakeholders are becoming irritated.

| Turn | Tell Players | Background | Injects |
|---|---|---|---|
| Pre-incident | Staff members have begun receiving calls from customers complaining about being unable to use important services. | A paid stressor service (hired by cyber criminals) is performing a DDoS attack against the organisation in the hopes of extorting Bitcoin (replace if not relevant to organisation).<br><br>The DDoS attack is targeting the organisation's website. The network traffic contains malformed HTTPS and is mostly coming from neighboring countries. | None this turn. |
| Incident declared | Staff members are receiving calls, emails, and messages complaining about outages. | The DDoS attacks continue. As a result, customers are getting agitated. Some senior staff members are now aware of the incident.<br><br>The criminals have sent an email demanding payment. | **Inject 11:** A senior staff member receives an email from the criminals demanding the company pay (D20) Bitcoin to stop the DDoS attack.<br><br>**Inject 8:** Attacker sends an email to you including screenshots of social media complaints from your customers and threatens more cyber attacks if demands are not met (PRIVATE NOTE: GENUINE) |
| Recovery | The DDoS attack has ceased.<br>Senior leadership and the important stakeholders are requesting an incident summary. | The attack has concluded.<br>Media articles about your organisation's DDoS attack are circulating online. | **Inject 6:** An important stakeholder/board member calls for status |

## Ransomware

Difficulty level: 

**Scenario Code**: *1456 (Extra Inject: 13)*

**Description:** Ransomware attack by hired security testers. Admin laptop compromised, user reported that machine boots into ransomware screen. Low-profile USB drive in one of the ports.

| Turn | Tell Players | Background | Injects |
|---|---|---|---|
| Pre-incident | A member of staff has contacted IT, reporting that their machine is booting into a ransomware screen.<br><br>They have admin privileges.<br><br>The machine was working fine in the morning, user only noticed the issue after lunch.<br>No other reported issues. | A security tester, hired by the business, has managed to gain access to the office area used by staff with admin privileges.<br><br>They have inserted a low-profile USB stick into one of the admin laptops while the user was away.<br><br>It has a ransomware payload, which has just deployed. The drive has been encrypted, but no data is being exfiltrated. | None this turn. |
| Response phase | The staff member is panicking, worried they are going to lose their job. They keep coming to IT to ask if there's been any progress.<br><br>More users are reporting that their machines now have the same ransomware screens. | The tester is still in the building, and has managed to infect D6 more machines.<br><br>The tester will leave later this turn. | **Inject 13:** Hot backups do not work. Offsite backups will take (D6) hours to retrieve. |
| Recovery | Fast-forward one week. Management discloses to the team that the ransomware event was part of a security test. | The test has concluded. | None this turn. |

## Cloud Infrastructure Compromise

Difficulty level: 

**Scenario Code**: 6244 (Extra Injects: 12, 18)

**Description:** The organisation's cloud infrastructure has been compromised by an attacker, leading to exfiltration of PII and unwanted media attention.

| Turn | Tell Players | Background | Injects |
|---|---|---|---|
| Pre-incident | The organisation's IT administrators have received an email from law enforcement notifying you of malicious connections to your cloud infrastructure. | The organisation's cloud infrastructure was compromised due to a misconfiguration (exposed access keys).<br><br>The attacker has used this access to access a hosting bucket, downloading PII data on customers. | None this turn. |
| Response phase | A staff member finds a screenshot on social media showing PII from the organisation's customers. | The attacker has begun leaking samples of the PII on a darknet forum and is offering to sell the full dataset to anyone online. Screenshots of these samples are being posted on social media.<br><br>The attacker continues to have access until they are removed and prevented from regaining access (e.g. access key is rotated, and the misconfiguration is fixed). | **Inject 12:** A staff member finds an email from months ago in which a researcher details the misconfiguration (exposed access keys).<br><br>**Inject 18:** A media outlet has released an article outlining the incident and critiquing the organisation's data collection and privacy practices. The article cites an anonymous source within the company. |
| Recovery | No further information (You may want to provide a summary of the current state of the attack). | The attacker continues to have access until they are removed and prevented from regaining access. | None this turn. |

# Scenario Builder

This Scenario Table allows Facilitators to quickly generate novel infrastructure-related incidents for teams to participate in. To use, simply roll a six-sided die four times and select the options provided in each column corresponding to each die rolled. Alternatively, you can just choose a specific type of incident and each of its aspects manually. Further general-purpose injects are provided in the next section.

**Reminder:** Players only start the game knowing information based on the **Discovered By** column. The rest of the information is made available from the Facilitator as the incident progresses, resulting from player actions and injects.

**Incident Type (first D6):** this is the general type of incident for the scenario.

**Discovered By (second D6):** this is how the players first find out about the incident. The amount of detail provided is at the discretion of the Facilitator. For instance, 'internal monitoring' may be an alert that identifies the type of incident. Alternatively, an alert may simply identify suspicious network traffic.

**Vector (third D6):** the attack vector used by the attackers to enter the system or otherwise cause the incident. This information will generally be disclosed to players as the game develops. Facilitators can use their discretion as to when they want to disclose this information.

**Specific Injects (fourth D6):** specific injects add layers designed to help develop the incident. Facilitators can use their discretion as to when they want to disclose this information, depending on how quickly they want to progress the game. Sometimes the specific inject might be part of the pre-incident information (e.g. a ransomware screen on boot) or it could happen as the team responds to the incident (e.g. the user has now called the helpdesk back and is reporting a ransomware screen on booting up their device.)

**Extra Injects:** the Facilitator can decide at any time when to play these. They could be used to add pressure to the response team, to make the players think about another aspect of response, or to distract players from their original goal.

# Scenario Exercise: Infrastructure

| Incident type (D6) | Discovered by (D6) | Vector | Specific injects |
|---|---|---|---|
| (1) Malware/ Compromised machine | (1-3) Internal monitoring<br>(4-6) User noticed strange behaviour | (1) Phishing<br>(2) Malware document<br>(3) Downloaded by user looking for freeware<br>(4) Friends/family borrowed machine<br>(5) USB device<br>(6) Unknown | (1) User has a history of installing browser toolbars<br>(2) User has multi-factor authentication turned on<br>(3) API keys are involved -- Github & AWS<br>(4) Security testers were here at the time of the event<br>(5) Antivirus has quarantined a file in their downloads folder<br>(6) Their computer gives a ransomware screen on boot |
| (2) Compromised user account | (1-2) Internal Monitoring<br>(3-4) External Provider Notification<br>(5-6) User Noticed Strange Behaviour | (1) Unknown<br>(2) Phishing<br>(3) Password spraying<br>(4) Keylogger<br>(5) Public machine usage<br>(6) Password written down | (1) User password is listed in HaveIBeenPwned<br>(2) User has multi-factor authentication turned on<br>(3) API Keys are Involved (Github & AWS)<br>(4) Security testers were here at the time of the event<br>(5) Antivirus has quarantined a file in their downloads folder<br>(6) Machine gives a ransomware screen on boot |
| (3) Individual server or system | (1) Internal monitoring<br>(2) Law enforcement<br>(3) Vendor/partner<br>(4) Staff noticed strange behaviour<br>(5) Complaints from customer<br>(6) Online claims by attacker in media | (1) Web shell<br>(2) Remote file include<br>(3) 3rd party Javascript<br>(4) Out-of-date software exploit<br>(5) Zero-day exploit<br>(6) Backdoored dependency/plugin | (1) The compromise allegedly occurred (D20) months ago<br>(2) The server processes personally identifiable data<br>(3) A configuration error exposed an old backup of the server database<br>(4) You recently migrated from an on-premises to cloud environment<br>(5) The servers were rebuilt (D20) months ago<br>(6) The server's antivirus/anti-malware alerted to an existing infection (D20) months ago:<br>(1-2) Related<br>(3-4) Unrelated<br>(5-6) Unknown if related |

| Incident type (D6) | Discovered by (D6) | Vector | Specific injects |
|---|---|---|---|
| (4) DDoS | (1) Internal monitoring<br>(2) Vendor/partner<br>(3) Staff noticed strange behaviour<br>(4) Complaints from customers<br>(5) Callouts on socials directing users to LOIC<br>(6) Online claims by attacker in media | (1) Botnet ping flood<br>(2) Spoofed IP address (reflection attack)<br>(3) IP fragmentation attack<br>(4) LOIC/other crowdsourced brigade<br>(5) Paid stressor service<br>(6) Malware (fork bomb) | (1) The attack started at (D20) hours (24-Hour Time)<br>(2) Targets public-facing website<br>(3) Targets back end/infrastructure<br>(4) Targets VPN service<br>(5) The attacker attempts to sidestep mitigation (Such as by changing source IPs)<br>(6) The organisation receives a threat stating that the DDoS attack was only 'a warning' and there would be a larger attack if (D6) Bitcoin was not paid. |
| (5) Domain admin compromise | (1-2) Internal monitoring<br>(3-4) Extra accounts found<br>(5-6) User noticed strange behaviour | (1) Unknown<br>(2) Insider<br>(3) Password cracked<br>(4) LLMNR/MDNS attacks<br>(5) Malware on domain controller<br>(6) Service account compromise | (1) An unexpected and unknown domain admin account has been found. It is actively logged into a machine<br>(2) Unauthorised remote access found in logs<br>(1-2) A server has been found with Teamviewer<br>(3-4) RDP was found internet-accessible on the original system<br>(5-6) A server was found exfiltrating unknown data to overseas IP<br>(3) Security testers were onsite at the time of the event<br>(1-3) Confirmed they left new accounts after testing<br>(4-6) This is outside the scope of their testing<br>(4) Security testers were here at the time of the event<br>(5) Antivirus has quarantined a file in their downloads folder<br>(6) Domain controller now gives a ransomware screen on boot |
| (6) Cloud infrastructure compromise | (1) Internal monitoring<br>(2) Law enforcement<br>(3) Vendor/Partner<br>(4) Staff noticed strange behaviour<br>(5) Media runs story based on anonymous tip<br>(6) Online claims by attacker in media | (1) Keys exposed in public code<br>(2) Admin account compromised<br>(3) Cloud tenant system compromised<br>(4) Bad configuration allows public resource access<br>(5) Cloud provider compromised<br>(6) Unknown | (1) Billing notification from cloud provider<br>(2) Strange activity notification from cloud provider<br>(1-2) Port-scanning others<br>(3-4) DDoSing others<br>(5-6) Botnet command and control<br>(3) Bitcoin miner found on device<br>(4) Hosting service's bucket publicly accessible<br>(1-2) Contains pseudonymised PII data<br>(3-4) Contains raw personal data<br>(5-6) Contains non-sensitive data<br>(5) Full data lake access possible<br>(6) Build system affected |

# Extra Injects

This table features a range of optional, general-purpose injects that can be activated at any time during the scenario. They can be selected by rolling a D20.

| ID | Description |
|---|---|
| 1 | Sudden resignation of related staff member |
| 2 | Malware detection (PRIVATE NOTE: FALSE POSITIVE) |
| 3 | Malware detection (PRIVATE NOTE: GENUINE) |
| 4 | Surprise media enquiry asking for information on alleged cyber outage |
| 5 | Stakeholder calls for status (PRIVATE NOTE: SCAMMER) |
| 6 | Stakeholder calls for status (PRIVATE NOTE: GENUINE) |
| 7 | Sudden illness <random incident team person> Vulnerability was disclosed to the [organisation] via email months ago but has not been repaired or acknowledged by the organisation |
| 8 | Attacker sends an email to you including screenshots of social media complaints from your customers and threatens more cyber attacks if demands are not met (PRIVATE NOTE: GENUINE) |
| 9 | Internet connectivity is lost for (D20) minutes <DDOS attack> |
| 10 | Attacker claims to be a specific Advanced Persistent Threat and threatens more cyber-attacks if demands are not met (PRIVATE NOTE: SCAM, MADE-UP APT) |
| 11 | Email demanding payment of (D20) Bitcoin to an address to stop the attack |
| 12 | Vulnerability was disclosed to the [organisation] via email months ago but has not been repaired or acknowledged by the organisation |
| 13 | Hot backups do not work, off-site backups will take (D6) hours to retrieve |
| 14 | It emerges that this is part of a worldwide series of attacks through media reporting of similar incidents targeting organisations in similar industries. |
| 15 | Post appears on a web forum claiming that [organisation] has been compromised along with screenshots of data – this appears to be genuine data from the [organisation]. Attacker asks [organisation] for payment to prevent leak of data, otherwise attacker will sell data on the dark web. |
| 16 | [Organisation] has been contacted by one of its suppliers notifying them that they suffered a cyber attack. Facilitator to decide if relevant to this event or just coincidental. |
| 17 | Post appears on a web forum claiming that [organisation] has been compromised. Customer helpdesk starts to receive multiple calls from customers asking about the security of their information. |
| 18 | A media exposé alleging [organisation's] data collection and privacy practices are not good enough. The story quotes an anonymous source from within the company explaining [organisation] has suffered a cyber attack. (PRIVATE NOTE: if company has already made a public statement, the anonymous source claims the attack is worse than has been disclosed) |
| 19 | The company was hit with a very sophisticated malware/phishing attack last year, which the organisation resolved after calling in third-party response, and organisation considered this matter closed. The senior leadership want to know if this incident is related. FOR FACILITATOR: the incident is not related – this inject is designed to test messaging around assurance of systems. |
| 20 | An external repository was recently compromised - NPM, DockerHub, APT, etc. |

# Glossary

| | |
|---|---|
| **D6** | A six-sided die. This is used by the facilitator to set up the game, and to provide details for some of the injects. |
| **D20** | A 20-sided die. This is used by the players to set up the game, and to provide details for some of the injects. If you don't have access to a 20-sided die, there are applications available that provide this function. |
| **Facilitator** | The Facilitator drives the narrative and cadence of the event. They influence the groups decision-making ability by furthering the event through a series of prompts and by asking questions. |
| **Inject** | An unexpected event or action the Facilitator injects into the players turns to simulate a real-world scenario. |
| **Player** | A participant in *Rolls & Responders* who assumes any role and responsibility as agreed by the team. |
| **PRIVATE NOTE** | The inject should be played on the turn. The private note is supplementary information to be revealed at the discretion of the Facilitator either during the game or as part of the debrief. |
| **Tabletop** | A tabletop exercise is an informal, discussion-based session in which a team of players discuss their roles and responses to predetermined scenarios during an event. |

This page is intentionally left blank.

National Cyber Security Centre

PART OF THE GCSB