**MASTER EVENTS LIST**

**S-Unclass-Internal Cyber Attack-JS - 1.5 - 030-S\_TSL-Internal Cyber Attack-Unclass**

21/12/2022 09:09:25

# Monday 0900-1800

| Serial | Timing | Event | Description | Discussion | Responsible | Tasks & Data |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 5 mins | Business As Usual | Players get assigned roles, go over company policies and procedures regarding an internal cyber attack. | Ensure players review organisational chart, are familiar with channel, read content on scenario (Crawley Times Article, CEO email on mass layoff two months ago). |  |  |
| 2 | 5 mins | Crawley Office Reports Cyber Incident | SOC team and senior management contact you as the Incident Management Team to respond to an isolated cyber incident taking place in the Crawley offices - the Cyber Resilience Manager takes the lead and the InfoSec team provides you with updates. | What protocols would players usually follow in this case? Have players faced similar situations in the past? |  |  |
| 3 | 5 mins | Incident Management Begins | Players recieve more infomration confirming that there has been a malicious cyber attack on the Crawley Office. Players have to make decsions to manage the situation e.g. cut the network connection of Crawley office. | How do you ensure you're making the right decision? What else do you need to consider during this process? |  |  |

# Tues 0900 - 1800

| Serial | Timing | Event | Description | Discussion | Responsible | Tasks & Data |
| --- | --- | --- | --- | --- | --- | --- |
| 4 | 5 mins | Hacker Tweets About Attack | The hacker posts on social media that they are responsible for the attack. An influencer picks this up and spreads the tweet. Comms ask players for advice. | Is it too soon to react to this incident publically? |  |  |
| 5 | 2 mins | Hiring Forensic Specialist | CISO asks for players advice in hiring an external specialist. | Is there anything you need to be aware of in hiring an external specialist? |  |  |
| 6 | 5 mins | Damage to Customer Relations System Discovered | Press picks up the story and there is internal confusion regarding what has happened. Comms gets in touch to ask for more advice. | How do you communicate the event to your colleagues? What facts and details are you comfortable giving out pubically? |  |  |
| 7 | 2 mins | Comms Strategy | Twitter storm begins - comms asks for advise in responding to a journalist. | In dealing with journalists - do players have any concerns about what they say? |  |  |
| 8 | 2 mins | Hacker Identified As Former Employee | Your company have involved the police in the incident senior leadership have escalated the matter to a criminal investigation. | Do players have any advise on how situations like this would usually be dealt with? |  |  |
| 9 | 5 mins | Access to Crawley's Systems Restored | The malware is contained in Crawley's network to the extent that staff are able to use their access again. The management of the incident is almost complete. | What information is missing? what else do you want/need to know? |  |  |

# Weds 09:00-1800

| Serial | Timing | Event | Description | Discussion | Responsible | Tasks & Data |
| --- | --- | --- | --- | --- | --- | --- |
| 10 | Up to facilitator | Recovery Begins | Specialist details how long the full recovery process will take, how much it will cost, customer relations asks for advise in communicating resolution with customers. | Are players happy with this cost? What else should be considered? |  |  |
| 11 | Up to facilitator | Communications/Head Office Ask for Press Release | The Communications team are putting together a press release to update your customers and the public about what has happened and what is being done to resolve the access issues. They want the players' input. | How do you communicate what happened to the Press? |  |  |
| 12 |  | End of Exercise |  |  |  |  |