Incident handler's journal

Date: 28/05/2024	**Entry:** 01
Description	A health organisation’s business operations were disrupted by a security incident where a phishing email attachment was downloaded which caused ransomware to install. This ransomware encrypted the organisations files and a unethical hacker group left a note saying the organisation was hacked by them and that their files were encrypted. They also asked for money in exchange for the decryption key.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? - The incident was caused by a group of unethical hackers. • **What** happened? - A phishing email was accessed by an employee and the attachment of the email was downloaded causing ransomware to install on the computer and causing the organisation's computer files to be encrypted. • **When** did the incident occur? - The incident occurred on Tuesday at 9:00am. • **Where** did the incident happen? - At a small U.S health care clinic. • **Why** did the incident happen? - The incident happened as a group of ethical hackers sent a phishing email to an employee. The employee did not realise the email was illegitimate and hence downloaded the file.
Additional notes	The clinic should train all their staff on how to identify phishing emails if they have not already. In addition to this, the clinic should look into upgrading some

	of their cybersecurity frameworks and policies.

Date: 28/05/2024	**Entry:** 02
Description	SQL was used to filter data
Tool(s) used	SQL filtering with AND, OR and LIKE operators
The 5 W's	**N/A**
Additional notes	Include any additional thoughts, questions, or findings.

Date: 28/05/2024	**Entry:** 03
Description	Linux file permissions and folder permissions changed to respond to a cybersecurity incident.
Tool(s) used	Linux and chmod command
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? - an unethical hacker

	• **What** happened? - a hacker gained access to a website servers source code • **When** did the incident occur? - 28/05/2024 • **Where** did the incident happen? - At a software company • **Why** did the incident happen? - The source files were not configured to reject read and write permissions for other users.
Additional notes	Include any additional thoughts, questions, or findings.

Date: 27/05/2024	**Entry:** 04
Description	Created a controls and compliance report for a Toy Store
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	N/A
Additional notes	Include any additional thoughts, questions, or findings.

Completed by Yedukondalu Alias Rasavihari Markonda Patnaikuni on the 28th of May 2024