Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: Incident occurred on a Tuesday at ~9:00 AM	**Entry:** Entry #1
Description	Ransomware attack on a small U.S. primary-care clinic. At ~9:00 AM on a Tuesday employees reported inability to access medical records and other files; ransom note was displayed on endpoints. Business operations were disrupted and computer systems were shut down.
Tool(s) used	List any cybersecurity tools that were used. • Email gateway • Endpoint detection • SIEM • network monitoring • Backup system
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident?

	○ An organized criminal group (threat actor) known to target healthcare and transportation industries. They gained entry via targeted phishing. ● **What** happened? ○ Targeted phishing emails delivered a malicious attachment. When opened, malware installed on endpoints and the attackers deployed ransomware that encrypted critical files and displayed a ransom note demanding payment for a decryption key. Employees could not access patient records — operations stopped. ● **When** did the incident occur? ○ Tuesday morning at approximately 9:00 AM (exact calendar date not provided). ● **Where** did the incident happen? ○ On the clinic's internal IT environment — employee endpoints, likely file servers or systems that host electronic medical records, and possibly network shares. ● **Why** did the incident happen? ○ Initial root cause: successful targeted phishing (malicious attachment). Contributing factors likely include one or more of the following: insufficient email filtering, lack of user awareness/training, insufficient endpoint protections or EDR gaps, inadequate network segmentation, and backups that were not isolated or tested.
Additional notes	Include any additional thoughts, questions, or findings. Patient care was disrupted due to inability to access electronic medical records (EMR). Activate contingency business continuity (paper charting, emergency workflows). Preserve evidence — this is crucial for forensics, insurance, and regulatory reporting.

	HIPAA/privacy regulatory obligations will apply — notify legal counsel and follow breach notification processes (also notify law enforcement and cyber insurer). Do **not** pay the ransom without consulting legal counsel and law enforcement; payment does not guarantee restoration and may have legal/insurance consequences.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes: Record additional notes.