



Incident handler's journal

Date: 1st August, 2023	Entry: #1
Description	A small U.S. health care clinic faced a ransomware attack on Tuesday at 9:00 a.m. The attack was done using a phishing email by an organized group of unethical hackers and now are demanding money for decrypting keys.
Tool(s) used	Not used
The 5 W's	<ul style="list-style-type: none">• Who caused the incident? An organized group of unethical hackers• What happened? Ransomware attack• When did the incident occur? Tuesday at 9:00 a.m.• Where did the incident happen? A small U.S. health care clinic• Why did the incident happen? Malware installed on employees' computers which was delivered using a phishing email. The intention behind this hack was financial gain.
Additional notes	Can this be protected in future? If yes, how.... Can we trust hackers to not ask for more money if the ransom is paid? Did the hackers get their hands on crucial stuffs which can be leaked? Can the business pay the ransom?

Date: Record the date of the journal entry.	Entry: Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. <ul style="list-style-type: none">• Who caused the incident?• What happened?• When did the incident occur?• Where did the incident happen?• Why did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	Entry: Record the journal entry number.
Description	Provide a brief description about the journal entry.

Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> • Who caused the incident? • What happened? • When did the incident occur? • Where did the incident happen? • Why did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	Entry: Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> • Who caused the incident? • What happened? • When did the incident occur? • Where did the incident happen? • Why did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	Entry: Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. <ul style="list-style-type: none">• Who caused the incident?• What happened?• When did the incident occur?• Where did the incident happen?• Why did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	Entry: Record the journal entry number.
Description	Provide a brief description about the journal entry.

Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> • Who caused the incident? • What happened? • When did the incident occur? • Where did the incident happen? • Why did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

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.
