Security Breach or Privacy Breach, Network Asset Protection/Non-Physical Business Interruption and Extra Expense, Cyber Extortion

A medical clinic insured sustained a cyber extortion event, involving the ransomware variant called Zepplin, resulting in the encryption of six of its servers, including its back-ups. The clinic lost access to all patient records and immediately notified its insurance company. The insurance company hired breach counsel to assist the insured, and IT forensics to determine whether the threat actor exfiltrated any records. Consultants were retained to negotiate the ransom payment in exchange for decryptor tools. IT forensics discovered that the records were not released, and as a result, patient notification was not required. In addition to the cyber extortion event, the clinic also sustained business interruption since it could not access patient files and see its scheduled patients during regular business hours.

Their cyber insurance paid for a total of $176,000 in expenses, which included:

- IT Forensics: $40,000
- Incident Response: $14,000
- Ransom Amounts: $30,000
- Breach Counsel: $24,000
- Business Interruption Loss: $68,000