Submit ONE PDF, answering these questions (the answers should be clearly delimited).

1. Compare and contrast the level(s) of transparency and timeliness in the incident response, any differences in incident handling you have detected (if any) between the Norsk Hydro and Travelex/Finablr cases. Should either of the two companies have simply paid the ransom demanded? If not, why not? [500 words, 20%]
2. To what degree do you think in the case of Finablr the cyber attack may have acted as an early warning sign, a kind of ‘canary in the coal mine’ for wider company governance standards, and possible IT investment deficiencies? In other words "should the events at Travelex have warned us that all was not well throughout the Finablr empire". [200 words, 10%]
3. Have victims learned the communications and crisis management lessons from Norsk Hydro/Finablr? Illustrate your answer with examples from two (ideally one good and one bad) ransomware attacks from 2023/4. [300 words; 20%]
4. More generally what risk does ransomware pose to your own business? If you don’t have a relevant business, frame your response in relation to a generic e-finance vertical market chosen exemplar, i.e. Invent a firm that sells financial products into some specialist market. It probably needs to be fairly visible and vulnerable for ransomware to be very effective (would the world notice if a firm that sold liability insurance to undertakers had problems?). I suppose one example might be pet insurance. [250 words, 15%]
5. Use a free [paid for ones may generate a better response, but this will make part 6 harder!] generative AI tool such as ChatGPT to answer the following question. “Learning the lessons from ransomware attacks is vital. Draw up an idealised incident response timeline (expressed in hours/days before/after D day, the day the attack actually takes place), identifying the target’s actions and responses to a ransomware cyber attack upon a generic fintech (e.g. e-banking ) provider. You should show adversarial actions too. (Both preparatory, initial launch and subsequent to the attack, hence the defence). So both attackers and defenders may well be doing things before D day. The target doesn’t pay the ransom immediately. The answer should be a table, with suitable annotated entries showing a maximum of 20 rows extending over a time period extending to no longer than two calendar months.”. You should submit your successful prompt (as well as the name of tool and the date of asking) and the answer you got. DO NOT EDIT THE ANSWER. [no word count, 5%]
6. Comment on the answer above, explaining where it is, or is not, good (in the sense of supported by the literature and/os examples) or bad (not supported, nonsense, contradictory etc.) [250 words, 30%]
7. Submit an annotated bibliography showing all references consulted (cross-reference these to each of the tasks above—aim to cite approx. 15-20 carefully chosen sources). By "annotated" I mean it's to explain WHY the article is in the bibliography. So there might be an article about an attack that was nothing like the ones you're writing about, but had a good analysis of the political factors behind allowing/banning ransomware payments, and the annotation might be "Used for analysis of general ransomware politics". That's the sort of length I am looking for, but of course an article might have more than one use, so you'd want to write more in that case.

N.B. The highlighted questions are Type C assessments.