1. What could have been done by the owners of Jebea to prevent the situation from happening?

So, the incident falls under Risk of security and fraud (04 Handout, p. 3) which is an external and preventable threat. To prevent this, Jebea's owners could have taken several proactive measures. First, they should have conducted a fraud risk assessment to understand their system's vulnerability to hackers and the effectiveness of their security measures. This assessment could have helped them identify potential weak points that cybercriminals might exploit. Second, upon the first reported incident, instead of dismissing it, they should have immediately launched an investigation and informed the relevant authorities, such as the Department of Information and Communications Technology (DICT), as this was now a legal and compliance issue. Finally, they failed in their duty to manage Reputational Risk (04 Handout, p. 3-4). By not addressing the initial complaint transparently and proactively, they damaged stakeholder trust. A proper response would have involved publicly acknowledging the issue, assuring users of an investigation, and temporarily taking the platform offline to fix the breach, thereby demonstrating that they value user safety and constructive feedback.

1. How can SWOT, TOWS, and PESTEL analyses address the threats that occurred on Jebea?

**SWOT Analysis**

This would have helped Jebea catalog its internal and external environment. The Threat (T) of "cybersecurity attacks from hackers" (04 Handout, p. 3) would have been a critical entry. A key Weakness (W) would have been "inadequate cybersecurity protocols" and "lack of a crisis communication plan." Identifying these formally would have made them a priority to address.

**TOWS Analysis**

**Maxi-Mini Strategy (ST)**: If a strength was "strong government partnership (DepEd)," they could have used that relationship to seek expert advice on cybersecurity from other government agencies (DICT) to minimize the threat of hacking.

**Mini Mini Strategy (WT):** To address the weakness of inadequate security and avoid the threat of hackers, they could have invested in robust cybersecurity software, hired IT security experts, and created an incident response plan.

**Pestel Analysis**

**Technological:** The analysis would force them to consider factors like "rapid evolution of cyber threats," emphasizing the need for continuous technological updates to their security.

**Legal:** It would make them aware of "data privacy laws" and "regulations on child protection online." Understanding these legal consequences would have compelled them to implement stricter security measures to avoid penalties and shutdowns, turning a potential threat into a guideline for compliance.

1. Think of one (1) technopreneurial enterprise that gives prime value to the safety of its client’s purchases, data, and privacy. How do you think the technopreneurial enterprise protects its clients’ information?

A prime example of a technopreneurial enterprise that gives prime value to client safety and data privacy is Apple Inc. Based on the principles in the handout, Apple likely protects its clients' information through a multi-layered approach that involves intellectual property and security risk management. Firstly, they heavily rely on proprietary innovations and trade secrets (04 Handout, p. 4), such as their unique encryption algorithms and secure hardware components like the Secure Enclave. These are protected legally through patents and non-disclosure agreements (NDAs) with employees. Secondly, they actively manage Security and Fraud Risk (04 Handout, p. 3). They employ rigorous fraud risk assessments to constantly test for vulnerabilities. Technologically, they use end-to-end encryption for services like iMessage and FaceTime, ensuring that even Apple cannot access the data. They also implement strict compliance with global data protection regulations (a PESTEL Legal factor), transparently informing users about data collection and giving them control over their information. This comprehensive strategy of using proprietary technology, continuous risk assessment, and strict legal compliance builds immense trust and differentiates them in the market.

**References**

<https://elms.sti.edu/files/10441789/04_Handout_1(3).pdf?lmsauth=080a65127215daa8ba0790219221fa5ced44566b>

<https://elms.sti.edu/files/10441789/04_Handout_2.pdf?lmsauth=4f7ee12a74d7b457adce5e6ca96228accf10fe84>