The Jebea Dilemma

Adrae Sotto
Audhy Montesa
Denver Patiag
Jean-Marc Vega
Jonathan Vargas
Justine Sirios
Mark Jello Millabas
Miggy Magbiray
Sean Mabbun
Thomas Pancha
Van Halen Viola

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

   There are many precautions the owners of Jebea should have taken to prevent this particular situation from occurring. In order to protect themselves from hacking attempts, the owners should have invested in robust cybersecurity measures from the beginning and immediately reported any hacking attempts to authorities. It is imperative that all security breaches are transparently disclosed to their user bases along with warnings and instructions not to access the content that is affected. When removing malicious content and securing their application, Jebea should work closely with cybersecurity experts during the investigation and cooperate fully with government agencies. Jebea should regularly update and audit its security protocols to prevent future vulnerabilities as well as, implement user authentication and content filtering mechanisms to ensure only safe and educational content is accessible. Implementing these measures could have assisted Jebea in preventing their regrettable circumstances and preserving the confidence of its user base and stakeholders.

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

   SWOT analysis would have helped Jebea identify internal strengths and weaknesses in its cybersecurity measures. TOWS analysis could have then enabled them to strategise by matching strengths to opportunities (e.g., expertise in technology education to address security threats) and converting weaknesses into strengths (e.g., enhancing cybersecurity protocols). PESTEL analysis would have allowed Jebea to anticipate external factors like regulatory changes and potential cyber threats. By combining these analyses, Jebea could have proactively strengthened its cybersecurity, sought government support, and aligned its strategies to mitigate threats. This holistic approach might have prevented the hacking incident and its devastating consequences.

2. **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?**

   One technopreneurial enterprise that prioritises the safety of its clients' purchases, data, and privacy is PLDT (Philippine Long Distance Telephone Company), a leading telecommunications and digital services provider in the Philippines. PLDT employs multiple security measures to protect client information. They invest heavily in advanced cybersecurity technologies, including firewalls, intrusion detection systems, and encryption protocols, to safeguard customer data from external threats. Regular security audits and vulnerability assessments are conducted to identify and address weaknesses. Additionally, PLDT educates its customers on safe online practices and offers two-factor authentication and data encryption options for added security. Continuous monitoring and quick response to security incidents ensure the integrity and confidentiality of client information.