1. The Data Privacy Act of 2012 protects personal information in the Philippines by ensuring that organizations collect, store, and process data responsibly and securely. Violations of this law can lead to identity theft, financial loss, and emotional harm for individuals, while organizations may face legal penalties, reputational damage, and loss of customer trust.

2. Zero Trust Architecture is a security model that requires continuous verification of every user, device, or system attempting to access a network, regardless of whether they are inside or outside the organization. This principle is essential today because cyber threats often originate from compromised internal accounts and devices, making perimeter-based security insufficient.

3. Security policies ensure consistent protection of information by guiding how employees handle systems and data. A Password Policy supports the CIA Triad by maintaining *confidentiality* through strong authentication, *integrity* by reducing unauthorized access and tampering, and *availability* by preventing account lockouts due to compromised credentials.

4. AI and ML improve cybersecurity by rapidly detecting anomalies, automating threat responses, and predicting attacks more accurately than manual methods. However, cybercriminals can also use AI to automate phishing, bypass defenses, and create more sophisticated malware, making attacks faster and harder to detect.

5. In a hypothetical breach where customer financial data is exposed, ethical issues include delayed breach reporting, lack of transparency, and inadequate protection of sensitive information. Transparency, accountability, and prompt incident response are critical because they help restore public trust and show that the organization is taking responsibility and mitigating harm effectively.