Emerging Cybersecurity and Data Privacy Threats

Bachelor of Science in Information Technology

Dimas, Christian Jay F.

September, 2025

Title: 85% of Philippine companies grapple with cyber threats – Cisco (2025)

Source: Inquirer.net (Adonis, 2025)

Summary of the Incident:

It reports on Cisco's Cybersecurity Readiness Index, which revealed that most companies in the Philippines faced cyber threats in 2024. The report showed that 85 percent of companies experienced AI-related cyberattacks. These included unauthorized account access and data poisoning, where data used by AI systems is altered to cause errors. The study also found that only 6 percent of local companies are fully prepared to handle these kinds of threats, while many employees are still not fully aware of the dangers.

Identified Threat/Vulnerability:

The main threats identified are unauthorized access, data poisoning, and the use of "shadow AI" or unapproved AI tools that are not regulated by the company. These threats are dangerous because they can lead to data theft, privacy violations, and disruptions in business operations. Many companies are also at risk because they have weak cybersecurity systems and are not ready to detect or stop advanced attacks.

Implications:

The effects of these threats can be serious. They can cause business disruptions, data leaks, financial loss, and reputational damage. On a larger scale, weak cybersecurity also poses risks to national security, especially if critical industries or government data are affected. The lack of readiness among many companies makes them easy targets for cybercriminals, which can harm not only the organizations but also their customers and employees.

Philippine Law Connection:

This issue is connected to Philippine laws. Under **RA 10175** or the **Cybercrime Prevention Act**, crimes such as hacking, unauthorized access, and identity theft are punishable. Under **RA 10173** or the **Data Privacy Act**, companies are required to protect personal information and use proper security measures. If personal data is stolen or systems are hacked due to poor protection, then these laws may apply. Even if this article did not name specific companies that violated the law, it shows that many organizations are at risk of non-compliance with these two acts.

Preventive & Mitigation Measures:

To prevent or reduce risks, companies should have stronger policies and rules on the safe use of AI. Employees must be trained to recognize and respond to cyber threats. Technical steps like using multi-factor authentication, monitoring accounts, and securing networks and cloud systems are also important. Companies should also prepare incident response plans so they can quickly act during an attack. Most importantly, they need to simplify and strengthen their security systems so they can properly detect and block threats.

Reflection:

In my opinion, even though companies know cyber threats are a problem, many are still not prepared to face them. New technologies like AI bring new risks, and old defenses are not enough anymore. Cybersecurity is not just about having advanced tools, it also requires

awareness, training, and strong policies. Philippine laws already provide guidelines, but companies need to act seriously in following them to protect both their data and their customers.

References

Adonis, M. J. (2025, May). *85% of Philippine companies grapple with cyber threats –Cisco*. INQUIRER.net. https://business.inquirer.net/524497/85-of-ph-companies-grappled-with-cyber-threats-in-24-cisco

Arellano Law Foundation. (2012). Republic Act No. 10175. Lawphil.net. https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html

Imperva. (2025). Cyber Security Threats | Types & Sources | Imperva. Imperva. https://www.imperva.com/learn/application-security/cyber-security-threats/

National Privacy Commission. (2012). Republic Act 10173 - Data Privacy Act of 2012. National Privacy Commission. https://privacy.gov.ph/data-privacy-act/