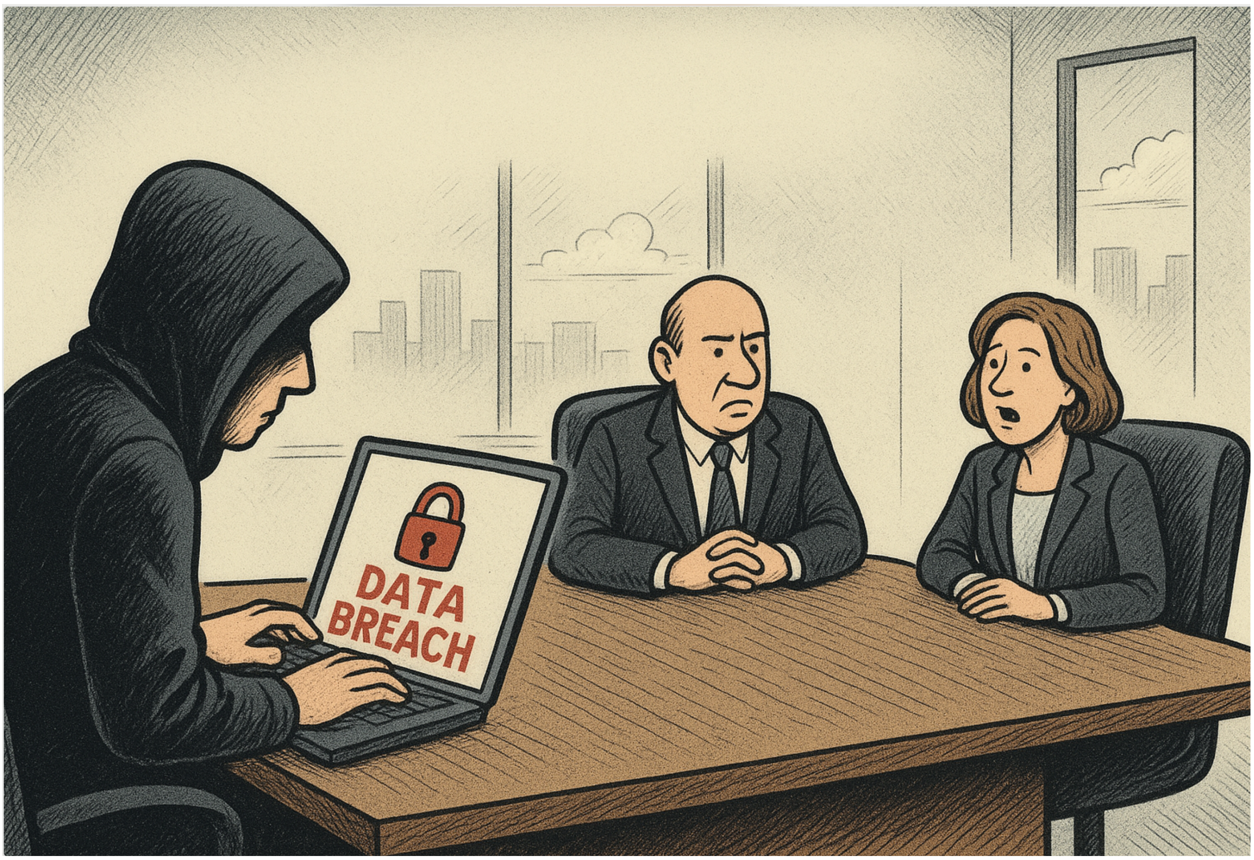
4 Minute Read | Cybersecurity & Society



From Data Breach to Boardroom: Why Cybersecurity is Now Corporate Governance

By: R A M Milanes

Cybersecurity is no longer a technical afterthought but a boardroom priority. In a world where digital transformation is accelerating, the consequences of personal data breach extend far beyond unauthorized exposure of sensitive personal information or data loss. Reputational damage, regulatory fines, shareholder lawsuits, and even personal liability for executives now accompany cyber incidents.

"Every cyber incident is not just an IT failure, it is a governance failure."

Cybersecurity as a Governance Issue

The digital economy has blurred the line between operational risk and corporate governance. Regulators now view weak cybersecurity as a sign of poor oversight.

Stakeholders interpret breaches as failures of leadership, not just failures of systems. For C-level leaders, the message is clear: cyber resilience is corporate resilience.

The Philippine Context

The Data Privacy Act of 2012 and the privacy regulator impose strict reporting obligations on personal data breaches. Failure to comply is increasingly seen as negligence. Shareholders and customers are beginning to demand transparency on cyber practices. For the first half of 2025 we saw the rise of AI-driven attacks in Southeast Asia which demonstrates that executives cannot rely solely on IT departments to safeguard the enterprise.

Why It Matters to the C-Suite

Reputation and Trust: In a relationship-driven market like the Philippines, reputational damage from a breach can outlast the technical incident.

Regulatory Exposure: Executives may face inquiries not only from regulators but also from boards and shareholders demanding accountability.

Business Continuity: Cyber incidents during critical operations such as banking transactions, retail sales, or logistics can paralyze entire supply chains.

Did You Know?

- 73% of Philippine executives say a major data breach would be “existential” for their company.
- The average cost of a personal data breach in the Philippines reached ₱85 million in 2024.
- Over 50% of local boards still do not have a cybersecurity committee.

4 Practical Tips for Executives

1. **Own cyber at the TOP** and elevate cybersecurity from IT to governance by integrating it into board agendas and risk committees.
2. **Demand metrics, never jargon**. Require dashboards that translate technical risks into business impact.
3. **Strengthen incident response** by ensuring crisis playbooks include board-level roles and communication strategies for all stakeholders especially events that fall into mandatory reporting.

4. **4. Embed cyber in culture.** Lead by example, align with values of trust and legacy, and make security part of daily business practice.

Cybersecurity is not just about protecting systems; it is about safeguarding governance, reputation, and trust. Every leader must recognize that cyber resilience is not delegated, rather it is directed.

"In the age of accountability, a cybersecurity breach is a leadership issue."