Governor SBP Speech for SBP-PBA Industry-wide Cybersecurity Drills - Awards Ceremony

January 23, 2026

Chairman Pakistan Banks Association,
Presidents, CEOs, and Chief Information Security Officers of banks,
Colleagues from across the banking industry and the State Bank of Pakistan,
Distinguished guests, Ladies and gentlemen

Assalam-o-Alaikum and a very good evening to you all,

It is a great pleasure for me to join you today at the awards ceremony, held to recognize institutions and individuals on successful completion of Pakistan's first-ever industry-wide cybersecurity drills for the banking sector. While the drill was designed to test our collective technical response capabilities, more importantly, it was set up to gauge the senior management's decision-making approaches during cyber crisis conditions. As you know, the exercise simulated coordinated cyber-attacks across one or multiple institutions and included scenarios that, if not managed effectively, could pose serious risks to the stability of the financial system.

Therefore, today's ceremony is not merely about distributing awards. It is about reinforcing a culture of preparedness, accountability, and leadership in cybersecurity. The institutions and individuals being recognized today have demonstrated a commitment that goes beyond regulatory compliance. They have invested in capability, coordination, and crisis readiness—qualities that are now indispensable for safeguarding financial stability in an era of persistent and sophisticated cyber threats.

The increasing interconnection and complexity of the financial system, combined with innovation and massive technology adoption, have introduced new risks and vulnerabilities. The threat actors today are no longer isolated hackers, but are highly skilled, well-resourced and organized. Moreover, rising geopolitical tensions have elevated the cyber threats and added further complexity by introducing another dimension to the cyber threat landscape. Moreover, the domestic scarcity of skilled cybersecurity professionals limits the ability of our institutions to effectively safeguard against cyber threats.

In this context, let me emphasize that cyber resilience cannot be achieved in isolation. It requires collective preparedness, transparent information sharing, and trust between regulators and regulated entities. In today's environment, cyber resilience is measured not by whether cyber-attacks occur, but by how effectively we respond to them.

As Pakistan's banking sector continues its digital transformation, maintaining public trust is paramount. Initiatives such as these cybersecurity drills send a strong and reassuring signal—to customers, markets, and international partners—that Pakistan's financial system is proactive, prepared, and aligned with global standards. This initiative is undoubtedly an important milestone—one that reflects the growing maturity, foresight, and collective resolve of our financial system to address significant emerging risks, such as cyber risks.

Ladies and gentlemen,

We at the SBP aim to uphold the international best practices when it comes to ensuring cybersecurity in the financial industry. Under our Strategic Plan – Vision

2028 – resilience, trust and stability are foundational pillars for our financial industry. And in today's highly digitalized and interconnected environment, cyber risk has emerged as one of the most significant threats to these pillars. It is no longer confined to IT systems or operational disruptions—it is a systemic risk with direct implications for financial stability, public confidence, and economic growth.

In recent years, SBP has taken several important measures to protect banks, financial market infrastructure, and—most importantly—our customers. We have established a dedicated Cyber Risk Management Department to strengthen supervisory focus on cyber risk within the banking sector. This department is enhancing supervisory methodologies, deepening engagement on the subject with our regulated entities, and strengthening incident reporting and response frameworks. Has the execution of these objectives been flawless so far? No, but we are moving in the right direction, and aiming to strike a workable balance between cybersecurity and operational efficiency, both within the SBP and in the broader banking industry.

To provide a clear strategic direction and roadmap to the industry for enhancing overall cyber resilience of the banking sector, we will, very soon, issue a comprehensive Cyber Resilience Strategy for our regulated entities. We are calling the strategy the "Cyber Shield 2025-30". This strategy will provide a forward-looking roadmap to enhance our financial sector's ability to identify, protect, withstand, and recover from cyber threats. It is built upon five foundational pillars namely: (1) strengthening cyber resilience, (2) maturing cybersecurity governance, (3) enhancing collaborations and partnerships, (4) developing cyber workforce and (5) continuously evolving the cybersecurity programs.

With that, I would like to commend all participating institutions for setting a new benchmark for industry collaboration and for jointly conducting the first industry-wide cybersecurity drills in Pakistan's banking history. I would like to offer a special thanks to the joint SBP-PBA committee – comprising officials from SBP and Chief Information Security Officers from MCB, Faysal Bank, Meezan Bank, UBL, Askari Bank, and BOP, who worked diligently during the past two years to plan and execute this cybersecurity drill. Also, congratulations to all award recipients.

I look forward to the insights and lessons that have emerged from this drill and how we go about collectively to embed them into our operations, and to seeing these exercises become a regular and integral pillar of our national cyber resilience framework.

Thank you.