Box 3.2: Building Systemic Resilience: The First Industry-wide Cyber Security Drill

The financial sector heavily relies on interconnected IT systems, essentially exposing it to cyber security risks. The disruptions in the event of a cyber-attack, that may turn systemic, will have considerable adverse implications for the stability of the financial system. At a time when the adoption and use of digital financial services is growing at an exponential pace in Pakistan, preparedness to take immediate and decisive action to mitigate a crisis and ensure a smooth flow of financial services becomes ever more critical.

Crisis simulation exercises (CSEs) are an integral part of forward-looking financial stability strategy and play a pivotal role in assessing pre-crises preparedness through identifying gaps and help strengthen fundamental components of financial stability. By simulating adverse scenarios such as liquidity shocks, market volatility, bank runs, operational disruptions, cyber incidents etc., these exercises identify vulnerabilities and strengthen contingency planning through enhancing coordination, institutional learning, and systemic resilience.

Once viewed as an operational issue, cyber risk now poses cross-border financial stability risks. The World Economic Forum's Global Risks Report 2025 identifies cyber espionage and warfare among the top near-term risks, while the Bank for International Settlements and the Financial Stability Board emphasize cyber resilience as critical to global stability. Domestically, the State Bank of Pakistan's 17th Systemic Risk Survey (January 2026) identifies cyber security as one of the significant risks to the financial system. Strengthening cyber resilience through robust standards, coordinated regulation, and integration into macroprudential frameworks is therefore essential to preserving financial stability.

Acknowledging the criticality of cyber risk, the Coordination Committee of SBP and Pakistan Bank Association (PBA) resolved to undertake a dedicated industry-wide cyber security simulation exercise. Subsequently, Pakistan's first ever industry wide cyber security drill was conducted in January 2026 through a dual-track approach comprising both technical and management drills. The coverage of the exercise was broad including thirty-four financial institutions, which comprised all Commercial/Islamic/Digital banks as well as major PSO/PSP viz. 1-Link and NIFT. The well-coordinated cyber drill assessed technical readiness, decision making and management readiness for crisis response.

- The *technical drill* was intended for Incident Responders – Security Operation Centre (SOC) Analysts, threat hunters and Incident Response (IR) teams, with the objective of detecting, investigating, and responding to simulated cyber-attacks.
- The *technical decision-making exercise* was designed for senior IT and Information Security personnel to test incident response procedures and decision-making capabilities under high-pressure scenarios.
- Participants in the *management drill* also included C-Suite executives who are part of their respective crisis management teams. This exercise assessed time-critical strategic decision making, public relations handling, business continuity activation and regulatory engagement.

The hypothetical crisis scenario was structured to simulate a sophisticated cyber incident resulting in material disruptions to critical digital channels and key third-party service providers. The drill required both technical and senior management functions to operate in a coordinated and disciplined manner, demonstrating robust analytical capabilities, cross-functional integration, and the capacity to take timely, risk-informed decisions under conditions of elevated operational stress. Participants were taken through a controlled and progressive escalation sequence, commencing with the detection of a security alert, advancing to the confirmation of an incident, and culminating in the declaration of an enterprise-wide crisis. This staggered approach provided clarity on escalation thresholds, decision rights, notification requirements, and governance protocols applicable at each phase of the event lifecycle. The simulation underscored the importance of effective communication, clearly delineated roles and responsibilities, and synchronized action across technology, operations, risk management, communications, legal, and executive leadership functions. By requiring coordinated engagement at tactical, operational, and strategic levels, the drill reinforced the imperative of institution-wide alignment and mature crisis management frameworks to safeguard operational resilience, continuity of critical services in the face of evolving cyber threats to ensure financial stability.

The successful completion of the industry-wide cyber drill stands as a testament to the strong coordination and effective collaboration among all participating stakeholders. This achievement underscores the financial sector's commitment to safeguarding the integrity, confidentiality, and availability of critical financial systems and services.

The drill further demonstrates the industry's collective resolve to remain proactive, adaptive, and resilient in navigating an increasingly complex and dynamic cyber threat landscape.

Going forward, and in line with recommendations of the International Monetary Fund, the SBP intends to institutionalize a systematic, multi-year cyber drills program, aligned with internationally recognized best practices, including the G-7 Fundamental Elements of Cyber Exercise Programmes, to ensure a structured, consistent, and progressively maturing approach to cyber resilience testing across the financial sector.