EXTENDED SUMMARY

This study examines the complex landscape of cybersecurity incident notification obligations in Turkey, analyzing the theoretical foundations, practical implications, and optimal design of multi-layered reporting architectures through the lens of risk governance, decentered regulation, and meta-regulatory frameworks.

Turkey's cybersecurity notification regime has entered a new phase with the enactment of the Cybersecurity Law (Law No. 7545), establishing the Cybersecurity Presidency (SGB) as a central coordinating authority. However, this new framework does not replace existing sectoral notification mechanisms maintained by regulatory bodies including the Information and Communication Technologies Authority (BTK), the Banking Regulation and Supervision Agency (BDDK), the Capital Markets Board (SPK), the Energy Market Regulatory Authority (EPDK), and others. This creates a situation where the same cybersecurity incident may trigger multiple, parallel reporting obligations to different authorities, each with distinct timelines, formats, and thresholds. The research question centers on how this polycentric notification architecture can be optimized to balance regulatory effectiveness with compliance burden.

The analysis draws on three interconnected theoretical perspectives. Risk society theory explains why cyber risks inherently defy singular regulatory categorization. Modern cyber risks exhibit characteristics that transcend traditional boundaries: they are spatially and temporally unbounded, often invisible without technical expertise, potentially irreversible in impact, exceed conventional liability frameworks, and challenge democratic decision-making processes. This multi-dimensional nature means that a single incident simultaneously constitutes an operational continuity issue, a data protection breach, a financial stability risk, and potentially market-sensitive information. Decentered regulation theory demonstrates that regulation emerges not from a single hierarchical authority but from complex interactions among multiple actors, knowledge flows, and power relationships. Different regulatory communities operate with distinct rationalities: BDDK approaches cyber incidents through financial stability metrics; BTK focuses on network infrastructure resilience; SPK evaluates market transparency implications; KVKK safeguards fundamental rights related to personal data. Meta-regulation and coordinated pluralism concepts provide the normative framework for

addressing coordination challenges without sacrificing the benefits of polycentricity, establishing common standards and information-sharing protocols while preserving sectoral autonomy.

The study maps detailed notification requirements across sectors. The Cybersecurity Law mandates "without delay" notification to SGB for detected vulnerabilities or cyber incidents. BDDK requires immediate reporting through cyber incident management procedures. SPK demands "immediate" notification under its Information Systems Management Communiqué and public disclosure through the Public Disclosure Platform for material events. BTK stipulates reporting breaches affecting more than 5% of subscribers "as soon as possible." KVKK establishes a 72-hour deadline for personal data breach notifications. TCMB requires "immediate" notification for payment system incidents. EPDK employs a maturity-level-based differentiated obligation system. This multiplicity creates three categories of problems: definitional inconsistencies where the same incident receives different classifications, temporal conflicts between vague terms and specific deadlines, and format diversity requiring duplicate data entry across separate reporting systems.

The European Union's approach offers instructive solutions. The NIS2 Directive establishes a standardized three-stage timeline: early warning within 24 hours, incident notification within 72 hours, and final report within one month. Commission Implementing Regulation 2024/2690 provides quantifiable thresholds for determining incident significance, including financial loss exceeding €500,000 or 5% of annual revenue, service interruptions lasting more than 30 minutes, and impact affecting at least 5% or one million EU users. The Digital Operational Resilience Act demonstrates sector-specific consolidation, explicitly amending the Payment Services Directive 2 to channel all ICT incident reporting through DORA's framework, thereby eliminating duplicate reporting. The Cyber Resilience Act establishes a single reporting platform operated by ENISA for product vulnerabilities, showing how specialized domains can benefit from unified channels.

The study proposes an integrated notification framework based on meta-regulatory principles, operating through a single-entry-multiple-exit architecture. Operators would submit a unified report through SGB's centralized portal using a common data dictionary. Intelligent routing mechanisms would automatically distribute relevant information to appropriate

sectoral authorities based on incident classification. The framework incorporates three essential components: a common data dictionary standardizing terminology while accommodating sector-specific data fields, a minimum common dataset including incident detection time and affected systems, and sector-specific modules allowing each authority to request additional information relevant to its regulatory perspective. Risk-based tiered reporting implements a three-stage process with initial notification for situational awareness, detailed notification with comprehensive analysis, and final reports documenting remedial actions and lessons learned. The SGB's role evolves from parallel regulator to meta-regulator, coordinating sectoral mechanisms rather than directly managing all notifications. Certain notification channels remain separate due to distinct protected interests: KVKK's fundamental rights protection and KAP's investor protection functions serve different legitimacy bases than operational risk supervision, warranting independent mechanisms with coordination protocols.

The study demonstrates that Turkey's multi-layered cybersecurity notification regime reflects not regulatory dysfunction but the inherent multi-dimensionality of cyber risk. Parallel obligations arise from different epistemological communities evaluating the same incident through distinct analytical frameworks. The Cybersecurity Law's secondary regulation authority provides the legal foundation for implementing coordinated notification architecture through common data dictionaries, standardized timelines aligned with international best practices, quantifiable thresholds for incident classification, and automated information-sharing protocols, achieving effective cyber risk governance without sacrificing sectoral expertise.