International Journal of Cyber Law

Ransom Ware Corporate Governance, and the Law A Case for Reclassification Under PECA 2016

Khadeeja Ahmad Hussain[1*]

[1] Lahore Leads University, Pakistan
* *khadijaahmadhussain123@gmail.com*

ABSTRACT

Ransom ware has evolved from an individual cybercrime into a significant corporate governance risk. This research examines how legal systems should reclassify ransom ware within corporate risk frameworks. It focuses specifically on Pakistan's Prevention of Electronic Crimes Act, 2016 and proposed amendments. The study aims to analyze fiduciary duty, board accountability, and mandatory incident reporting obligations. It uses a qualitative research design, applying doctrinal analysis and document analysis throughout. Data was drawn from scholarly literature, official legal texts, and recent policy publications. Findings show that current laws inadequately address corporate-level ransom ware liability and reporting gaps. Boards often lack clear guidance for meeting cyber security governance responsibilities under existing law. The research recommends institutional reform, phased implementation, and clearer statutory definitions for ransom ware. It also suggests balancing corporate obligations with fundamental digital rights protections carefully. These findings support treating ransom ware as a governance priority requiring coordinated legal reform. The study concludes that modernizing corporate cyber law strengthens accountability and national resilience together

Keywords: *Pakistan, Ransom Ware, Corporate Risk, Cyber Law, Fiduciary Duty, PECA 2016, Case Law*

HOW TO CITE THIS ARTICLE (APA 7th Edition)

Hussain, K. A. (2026). Legal Reclassification of Global Ransom Ware as Corporate Risk. *International Journal of Cyber Law*, *1*(2), 1–14. https://doi.org/10.59022/IRSHAD-iijcl.11

I. INTRODUCTION

Ransom ware attacks now strike a business every few seconds worldwide. This is not a small technical problem anymore. It has become a major corporate risk with legal consequences. Companies lose money, data, and customer trust after an attack. Courts and regulators are now asking hard questions about accountability. Who is legally responsible when a ransom ware attack causes harm to third parties? Is it only a cyber security issue, or also a governance failure? Insurance companies are also rethinking how they price and cover these risks. This shift reveals a bigger legal problem underneath the surface. Ransom ware is no longer just a criminal act committed by hackers. It is becoming a matter of corporate accountability and risk management law. Legal systems must decide how to properly classify this growing threat. The sections below explore this shift in careful detail, since reclassification directly affects liability rules, insurance contracts, and regulatory oversight (Baker & Shortland, 2023).

Began as a criminal nuisance affecting individual computer users decades ago. Over time, attackers shifted focus toward large corporations and critical infrastructure systems. Early legal frameworks treated these attacks purely as criminal matters for police. Corporate law rarely addressed ransom ware as a boardroom governance concern. Scholars mostly studied ransom ware through technical or criminological lenses at first. Legal scholarship on corporate liability for cyber incidents remained thin for years. Few studies examined whether directors owe fiduciary duties around ransom ware preparedness. Regulators also lacked clear standards for holding companies accountable after attacks. This created a significant gap between technical risk and legal responsibility. Insurance markets evolved faster than corporate governance rules did in this area. Boards often escaped scrutiny even after major, preventable ransom ware incidents occurred. Recent research has started questioning this gap in accountability structures. This study builds on that emerging discussion about director liability and fiduciary duty (Frank et al., 2021).

We already know ransom ware causes serious financial and operational damage to firms. We also know regulators increasingly expect boards to manage cyber risk actively. However, the exact legal standard for board accountability remains unclear. Courts have not consistently defined what "reasonable" ransom ware preparedness looks like. This creates uncertainty for directors trying to meet their fiduciary obligations. It also creates uncertainty for regulators trying to enforce consistent standards. The problem, therefore, centers on this legal ambiguity around corporate risk classification. Without clear rules, boards may treat ransom ware as merely a technical issue. This research addresses that specific gap in legal classification and accountability. It asks how ransom ware should be formally reclassified within corporate risk law. It also asks what liability standards should apply to negligent boards. Answering these questions matters for investors, employees, and consumers alike. Clearer legal standards would strengthen corporate governance around cyber security threats. This shift is already visible in evolving boardroom governance practices (Gale et al., 2022).

Recent research shows growing consensus that ransom ware qualifies as a quantifiable enterprise risk. A systematic review found major gaps in reliable cyber risk data availability. Companies struggle to measure ransom ware exposure using consistent, comparable financial metrics. This data gap complicates efforts to require standardized corporate risk disclosure. Regulators want firms to disclose cyber threats clearly in financial statements. Yet without reliable data, disclosure requirements remain difficult to design effectively. This finding matters because disclosure directly affects investor decision-making and market trust. It also affects how courts evaluate whether a board acted responsibly. Poor data availability weakens legal arguments about foreseeable, preventable corporate harm. Scholars argue this gap must close before liability standards can mature. Better data would allow courts to assess reasonable care more precisely. It would also help regulators draft enforceable disclosure obligations for ransom ware. This finding directly supports treating ransom ware as material corporate risk (Cremer et al., 2022).

A second important finding connects ransom ware incidents directly to shareholder litigation outcomes. Empirical research reviewed multiple cases where breaches triggered formal governance failure claims. Shareholders increasingly sue boards after preventable ransom ware attacks damage company value. Courts are now examining whether directors ignored known cyber security warning signs. This shift signals a maturing legal theory around board-level ransom ware accountability. Litigation patterns show plaintiffs targeting inadequate risk oversight, not just technical failures. This distinction matters because it reframes ransom ware as a governance problem legally. Governance failures are easier to litigate than purely technical security lapses. Courts can evaluate board decisions using existing fiduciary duty frameworks already. This makes ransom ware liability claims more viable within corporate law systems. The research suggests litigation will keep shaping ransom ware risk classification going forward. Boards now face real legal exposure beyond reputational or financial damage alone. This growing body of evidence strengthens calls for formal legal reclassification (Liu & Babar, 2026).

Existing literature offers strong insight into disclosure gaps and shareholder litigation trends. However, these studies rarely examine consistent legal standards across different jurisdictions. Most research focuses narrowly on single countries or specific industry sectors. Few scholars have compared how courts define reasonable ransom ware preparedness globally. This leaves a clear gap in cross-jurisdictional legal analysis of corporate liability. Prior studies also stop short of proposing a formal risk classification framework. They identify governance failures but rarely suggest concrete regulatory reclassification models. This creates uncertainty about which legal category ransom ware should formally belong to. Future research must address how to standardize liability rules across borders. It should also explore how fiduciary duty precedents apply specifically to ransom ware. This study aims to fill that gap through comparative legal analysis. Addressing this gap will help courts and regulators reach a clearer conclusion, building directly on unresolved questions about corporate liability boundaries (Teichmann & Wittmann, 2022).

To examine how different jurisdictions legally classify ransom ware as a corporate risk.

To analyze existing fiduciary duty precedents applicable to ransom ware-related board liability.

To propose a comparative legal framework for standardizing corporate ransom ware liability across borders.

How should legal systems reclassify ransom ware as a formal corporate risk, and what standardized fiduciary liability framework should apply to boards across jurisdictions?

This research holds significant value for corporate boards, regulators, and legal scholars alike. It contributes new knowledge by clarifying ransom ware's legal status as corporate risk. Boards currently lack clear guidance on their fiduciary duties regarding ransom ware. This study offers a comparative framework that boards can practically apply. Regulators benefit because standardized liability rules improve enforcement consistency across jurisdictions. Investors also gain from clearer disclosure expectations tied to cyber security governance. Academically, this research fills a gap in cross-jurisdictional ransom ware liability scholarship. It extends existing literature by connecting governance disclosure to firm performance outcomes. Prior research shows cyber security disclosure directly affects financial performance in regulated sectors. This connection justifies treating ransom ware disclosure as a governance and legal priority. Society benefits when corporate accountability structures reduce preventable ransom ware harm broadly. Strengthening legal clarity ultimately protects employees, consumers, and shareholders from cascading damage, a link recent banking-sector evidence supports directly (Elsayed et al., 2024).

II. METHODOLOGY

This research uses a qualitative research design to examine legal reclassification of ransom ware. Qualitative methods suit legal research because law requires interpretation, not numerical measurement. The population for this study includes cyber laws relevant to corporate ransom ware risk. The specific sample focuses on Pakistan's Prevention of Electronic Crimes Act, 2016. This law directly addresses ransom ware, corporate liability, and mandatory incident reporting obligations. Data collection relied on scholarly literature and official legal documents rather than surveys. Keywords used to search databases included ransom ware, corporate risk, PECA 2016, and cyber security governance. Additional keywords included fiduciary duty, mandatory reporting, and cyber law amendment. These keywords guided searches across legal and multidisciplinary academic databases effectively. Official government websites provided verified legal texts for the current law itself. This included Pakistan's official legislative portal for accessing PECA 2016 provisions directly. Using official sources ensured accuracy when analyzing existing statutory language and amendments.

Validity and reliability were maintained by selecting recent, peer-reviewed scholarly publications throughout. Most sources included in this research were published within the last five years. This ensured findings reflect current legal thinking and evolving ransom ware threats. All laws referenced remain currently applicable and were verified against official legal texts. Authors of selected sources included legal scholars, researchers, and university-affiliated academics. This helped ensure credibility and academic rigor across all cited materials. Data analysis followed a doctrinal legal research approach throughout the entire study. Doctrinal analysis examines existing statutory text, judicial interpretation, and established legal principles directly. This research also applied document analysis to scholarly articles and policy papers. Document analysis involved systematically reviewing content, identifying themes, and comparing legal arguments. Together, these techniques allowed structured examination of both law and academic literature. This combined analytical approach supported the research objectives outlined earlier in this study.

Ethical considerations remained straightforward since this research used only publicly available documents. All scholarly articles, laws, and policy papers used were derived from public sources. Every reference used throughout

this research was properly cited to acknowledge original authors. This citation practice maintains academic integrity and avoids any unauthorized use of ideas. The researcher declares no conflict of interest throughout the entire research process. This study was conducted solely for academic and legal research purposes. Several limitations and delimitations should be acknowledged regarding this research's scope. Technology evolves rapidly, meaning ransom ware tactics may change faster than legal analysis. Cyber laws and policies can also be amended at any time. This creates a natural limitation regarding the long-term currency of specific findings. This research is delimited to Pakistan's legal framework, particularly the amended PECA 2016. Findings may therefore have limited generalizability to other national legal systems directly.

III. RESULTS

This section presents key findings on ransom ware's legal reclassification as corporate risk. It answers how ransom ware transitioned from individual crime to enterprise-level threat. It also examines existing gaps in board accountability and fiduciary duty standards. Small and midsized businesses face unique challenges compared to large corporations. Boards at smaller firms often lack dedicated cyber security expertise or resources. This creates uneven legal exposure across different company sizes and sectors. The findings below draw on recent legal and governance scholarship directly. They explore disclosure practices, litigation trends, and cross-jurisdictional liability standards together. Each finding builds toward a clearer picture of corporate ransom ware accountability. Together, they support the argument for formal legal reclassification of ransom ware. This section organizes findings around distinct themes identified in the literature. These themes connect directly to the research objectives outlined earlier. Understanding these findings helps clarify why governance gaps persist industry-wide. This groundwork sets up the discussion of implications in later sections, particularly for boards with limited resources (Opitz, 2018).

Ransom ware first appeared decades ago as a threat targeting individual computer users. Attackers demanded small payments to unlock personal files or devices. Over time, criminal groups shifted their focus toward larger, wealthier corporate targets. Businesses offered bigger payouts and more valuable, sensitive operational data. This shift transformed ransom ware from petty crime into organized corporate extortion. Attackers began targeting hospitals, banks, and critical infrastructure providers directly. Legal systems struggled to keep pace with this rapid transformation initially. Cyber law frameworks were originally designed around individual privacy and data protection. They were not built to address large-scale corporate operational disruption. Regulatory responses have slowly expanded to cover broader digital-age corporate risks. This evolution shows ransom ware now threatens entire business continuity, not individuals alone. Companies face reputational, financial, and legal consequences beyond simple data loss. This shift confirms ransom ware belongs within corporate risk and governance discussions today. Modern legal frameworks must reflect this evolving digital-age threat landscape (Lodhi et al., 2024).

IV. DISCUSSION

A. Corporate Ransom Ware Risk Management and Mandatory Incident Reporting

The Prevention of Electronic Crimes Act, 2016 was Pakistan's first major cybercrime law. It introduced penalties for hacking, malicious code, and unauthorized data access. Ransom ware falls under provisions addressing malicious code and system interference broadly. However, these provisions were written before ransom ware became a corporate-scale threat. Penalties often target individual offenders rather than systemic corporate vulnerabilities. The law lacks specific language addressing extortion through encrypted corporate data. This gap weakens deterrence against attackers targeting businesses rather than individuals. Courts must currently stretch general provisions to cover ransom ware-specific corporate harm. This creates inconsistency in how ransom ware cases are prosecuted nationally. Companies face unclear legal expectations regarding prevention and response obligations. An amendment could close this gap by defining ransom ware separately within PECA. It could also introduce corporate-specific deterrence measures absent from the original law. This foundational weakness justifies revisiting PECA's scope for modern corporate threats (Khadam, 2023).

Beyond definitional gaps, PECA 2016 also suffers from structural enforcement weaknesses. Investigative agencies often lack resources to handle complex ransom ware cases effectively. Cross-border attacks complicate enforcement further under the current legal framework. Jurisdictional limits prevent effective action against foreign-based ransom ware operators frequently. These structural issues were present since the law's original enactment. Scholars have long noted these gaps without seeing substantial legislative reform. This slow response leaves companies vulnerable despite growing ransom ware sophistication globally. An amendment addressing corporate risk

must also strengthen enforcement infrastructure directly. Simply adding definitions without enforcement capacity would achieve little practical change. Investigative training and cross-border cooperation mechanisms need explicit legal support. This structural gap remains central to understanding PECA's current limitations. Addressing it requires more than symbolic legislative updates alone. Real reform must pair definitional clarity with practical enforcement capability improvements (Iqbal, 2023).

Modern ransom ware attacks increasingly target Pakistani corporate and financial sector systems directly. Existing research shows PECA 2016 struggles to address these evolving threats adequately. The law's original framework did not anticipate large-scale corporate extortion schemes. Attackers now demand payments in crypto currency, complicating legal tracing and prosecution efforts. Corporate security teams often report incidents informally rather than through formal legal channels. This happens because reporting obligations under current law remain vague and inconsistent. Companies fear reputational damage more than they trust legal protection mechanisms. This creates a dangerous cycle where attacks go underreported and unpunished. An amendment mandating clear incident reporting could break this problematic cycle directly. It would give regulators accurate data on ransom ware frequency and impact. This data could then inform better-targeted corporate security policies nationally. Aligning PECA with contemporary corporate security challenges requires this reporting mechanism specifically. Without it, the law remains disconnected from real corporate threat patterns (Shabana & Rahman, 2024).

Cybercrime in Pakistan continues evolving beyond what PECA 2016 originally anticipated. Emerging threats like deep fakes now compound existing ransom ware and extortion risks. These overlapping threats demand a more comprehensive, forward-looking legal response. Current provisions were not designed to address hybrid, multi-layered digital attacks. Companies face combined risks from data encryption, impersonation, and reputational manipulation simultaneously. This complexity outpaces PECA's original, narrower cybercrime categories significantly. Legal responses must therefore expand beyond simple malicious code definitions. An amendment could introduce broader categories covering hybrid corporate cyber threats explicitly. This would future-proof the law against rapidly evolving attack methods. Regulators would gain clearer authority to address combined ransom ware and disinformation tactics. Without this expansion, companies remain exposed to threats the law cannot properly categorize. This evolving threat landscape strengthens the case for comprehensive legislative modernization. Pakistan's legal framework must adapt alongside these emerging digital-age corporate risks (Khan, 2025).

PECA 2016 also shows inconsistencies when compared against modern corporate risk frameworks. Enforcement challenges persist because the law prioritizes individual privacy over systemic risk. Corporate risk management requires proactive obligations, not just reactive criminal penalties. Current provisions focus heavily on punishing offenders after attacks occur. They offer little guidance on preventive corporate cyber security obligations beforehand. This reactive approach leaves companies without clear compliance benchmarks to follow. Regulators cannot easily assess whether a company met reasonable security standards. This ambiguity weakens both enforcement and corporate accountability simultaneously. An amendment could introduce preventive compliance requirements alongside existing punitive measures. This would align PECA more closely with international corporate risk governance standards. Such alignment would help Pakistani companies meet global cyber security expectations more easily. It would also reduce legal uncertainty during cross-border business operations significantly. These inconsistencies highlight why targeted amendment remains legally and practically necessary (Saleem et al., 2022).

The proposed amendment should mandate clear incident reporting timelines for affected companies. It should also require integration of risk management practices into corporate governance structures. Boards would need documented cyber security policies addressing ransom ware prevention specifically. This shifts accountability from purely technical teams toward board-level governance oversight. Regulatory bodies would gain authority to review corporate cyber security resilience regularly. This integration reflects broader global trends toward organizational cyber resilience requirements. Mandatory reporting would also improve national data on ransom ware frequency and cost. Better data supports more effective, evidence-based policy decisions going forward. Board-level accountability ensures cyber security becomes a governance priority, not an afterthought. This approach directly addresses gaps identified throughout Pakistan’s current cybercrime framework. It positions PECA as a modern tool for corporate risk regulation. Ultimately, this amendment would strengthen national resilience against evolving ransom ware threats. Such reform represents a necessary evolution in Pakistan's digital governance approach (Majeed et al., 2026).

B. Comparing Current Law and Proposed Corporate Ransom Ware Reforms

Current PECA 2016 provisions treat cybercrime primarily as individual criminal misconduct. The proposed reform shifts focus toward organizational accountability and systemic corporate risk. Existing law evaluates

cyberspace mainly through criminal prosecution and national security lenses. It rarely intersects meaningfully with corporate compliance obligations or governance structures. The proposed changes would directly embed compliance requirements within corporate operational practices. This marks a fundamental shift from punishment-focused law toward preventive governance regulation. Current provisions also lack integration with broader national cyber security policy objectives. Reform proposals aim to align corporate obligations with these wider policy goals. This alignment ensures companies operate within a coherent, unified regulatory ecosystem. Without such integration, corporate compliance remains disconnected from national cyber security strategy. The proposed amendment therefore closes this critical policy-law disconnect directly. Framing ransom ware as a systemic security threat supports this departure from the law's original, narrower legislative intent (Hansel, 2024).

Current law offers limited clarity on protecting critical infrastructure from ransom ware specifically. It does not clearly define which corporate systems qualify as critical infrastructure. This ambiguity weakens legal protection for essential financial and utility service providers. The proposed amendment would introduce clearer definitions covering critical corporate infrastructure explicitly. It would also mandate incident reporting specifically for infrastructure-related ransom ware attacks. This differs sharply from current law's general, non-specific reporting expectations. Mandatory reporting under the proposal would protect both corporate and national assets simultaneously. Current provisions treat all companies similarly, regardless of infrastructure importance or risk. The proposed reform would instead prioritize infrastructure-critical sectors for stricter oversight. This targeted approach represents a significant structural change from existing legal treatment. Companies operating critical infrastructure would face heightened compliance expectations under reform. This distinction did not exist within the law's original 2016 framework, a gap direct cyber security-act proposals for Pakistan aim to fill (Abdin, 2025).

Current law responds reactively to cyber threats after incidents have already occurred. It lacks proactive risk management requirements addressing ransom ware before attacks happen. Persistent ransom ware and cyber-espionage threats have exposed this reactive weakness repeatedly. The proposed amendment would require proactive risk assessments as standard corporate practice. This shifts legal expectations from reactive punishment toward preventive corporate responsibility. Current provisions rarely mandate ongoing security audits or risk evaluation processes. Reform proposals would require regular, documented cyber security risk assessments from companies. This creates measurable compliance benchmarks absent from the current legal framework entirely. Human and organizational weaknesses remain central to why companies stay reactive rather than proactive. Without proactive requirements, companies remain perpetually vulnerable to evolving ransom ware tactics. The proposed reform directly addresses this gap through mandatory preventive measures. This represents a strategic imperative missing from the law's original design (Kausar & Laghari, 2025).

Current PECA 2016 provisions offer minimal guidance on cross-border threat intelligence sharing. Ransom ware attackers frequently operate across multiple jurisdictions, complicating enforcement significantly. The proposed amendment would establish clearer protocols for cross-boundary information sharing. This addresses growing concerns about digital laws being weapon zed against legitimate security cooperation. Current law does not clearly distinguish legitimate threat-sharing from improper government overreach. Reform proposals would balance security cooperation with appropriate corporate privacy protections. This balance did not exist within earlier, less nuanced legislative language. Artificial intelligence now complicates cyberspace governance further, requiring updated legal frameworks. The proposed amendment would introduce provisions addressing AI-related ransom ware complications specifically. Current law remains silent on these emerging technological governance challenges entirely. This gap makes cross-border cooperation both legally uncertain and practically difficult. The proposed reform directly modernizes this outdated cross-jurisdictional legal approach (Allahrakha, 2024).

Current law traces its origins to Pakistan's earliest cybercrime legislative efforts. Those early efforts focused narrowly on defining basic cybercrime categories and penalties. They did not anticipate sophisticated corporate ransom ware extortion schemes emerging later. The proposed amendment builds directly upon these foundational, now-outdated legislative beginnings. It expands narrow original definitions into broader corporate liability and risk frameworks. Current law's foundational structure remains fundamentally individual-crime oriented rather than corporate-focused. This creates a persistent legal gap regarding organizational-level data breach responsibility. The proposed reform directly addresses this foundational gap through expanded corporate provisions. Early legislative groundwork did not consider board-level accountability for security failures. Reform proposals would introduce this accountability as a core legal requirement. This represents substantial growth beyond the law's original, narrower legislative scope. Comparative judicial doctrines from other jurisdictions support this expanded liability direction (Khawaldeh, 2026).

Current law provides limited guidance on determining corporate liability after data breaches. Courts must interpret general provisions broadly when assessing organizational responsibility for attacks. This creates inconsistent legal outcomes across different ransom ware-related corporate liability cases. The proposed amendment would establish clearer liability standards specifically for ransom ware incidents. It would define when companies bear legal responsibility for inadequate security measures. Current law leaves this determination largely to judicial interpretation without clear guidance. Reform proposals would reduce this uncertainty through explicit statutory liability standards. This directly benefits companies seeking clear compliance benchmarks for legal protection. It also benefits affected parties seeking accountability after preventable security failures occur. Current provisions were never designed to address these precedent-setting liability questions comprehensively. The proposed amendment fills this gap through targeted, ransom ware-specific legal standards. This distinction represents perhaps the clearest departure from current legal treatment (Ahmad, 2026).

C. Challenges in Applying Corporate Ransom Ware Risk Reforms

Enforcement capacity remains a major obstacle to applying stronger corporate cyber security obligations. Investigative agencies often lack technical training to handle complex ransom ware cases properly. Current penalties already struggle to deter individual offenders effectively under existing law. Applying stricter corporate deterrence measures requires significantly more specialized investigative resources. Many agencies simply lack funding for advanced digital forensics and tracing tools. Attackers frequently use crypto currency, making financial tracing especially difficult for investigators. Without better tools, new corporate deterrence provisions may remain largely symbolic. Building this capacity takes time, funding, and sustained institutional commitment nationally. Smaller investigative units may struggle most, given limited technical staff availability. This capacity gap threatens meaningful application regardless of how reform provisions are written. Strengthening deterrence requires parallel investment in enforcement infrastructure, not law alone. Comparative assessment confirms law enforcement capacity remains central to translating legislative intent into outcomes (Baloch & Abid, 2026).

Structural weaknesses within Pakistan's broader legal system also complicate effective application. Courts often lack specialized cybercrime benches equipped to handle ransom ware cases efficiently. Case backlogs already delay justice across many areas of Pakistani law. Adding complex corporate cyber security cases may worsen existing judicial system bottlenecks. Judges may also lack technical training needed to evaluate cyber security evidence properly. This creates risk of inconsistent rulings across similar corporate ransom ware cases. Structural reform within courts would need to accompany any new legislative changes. Without this parallel reform, new provisions may face slow, inconsistent judicial application. Emerging norms show enforcement gaps persist even where mandatory reporting duties exist. These challenges predate current reform proposals but remain highly relevant today. Successful application depends on addressing these underlying structural weaknesses directly. This governance gap remains a documented barrier across critical infrastructure sectors (Sharma et al., 2023).

Corporate compliance culture presents another significant challenge to effective law application. Many companies currently underreport ransom ware incidents due to reputational concerns. Even mandatory reporting requirements may face resistance from companies prioritizing public image protection. Building trust between corporations and regulators will take sustained, deliberate effort over time. Companies need assurance that reporting will not automatically trigger punitive regulatory action. Without this assurance, underreporting may persist despite new mandatory reporting obligations. Smaller businesses may also lack resources to implement required compliance infrastructure quickly. This creates uneven compliance capacity across different company sizes and sectors nationally. Larger corporations may adapt faster, leaving smaller firms disproportionately exposed to enforcement risk. Addressing this gap may require phased implementation timelines for smaller businesses specifically. Public sector preparedness evaluations confirm this cultural resistance remains a persistent implementation obstacle (Bhutta & Rashid, 2026).

Rapidly evolving ransom ware tactics also challenge the law's long-term practical effectiveness. Attackers continuously adapt methods faster than legislative processes can typically respond. This creates ongoing risk that legal definitions may quickly become outdated again. Regulators would need mechanisms for updating provisions without lengthy legislative reprocessing each time. Current legal frameworks generally lack flexible, adaptive updating mechanisms for emerging threats. Building this flexibility into new provisions represents a significant drafting challenge itself. Without it, the law risks repeating the same obsolescence problems seen previously. Emerging threats require continuous legal monitoring and periodic provision reassessment going forward. This demands sustained institutional attention beyond simply passing new legislation once. Many jurisdictions struggle with this ongoing adaptation challenge, not just Pakistan alone. Comparative index-based analysis confirms Pakistan lags behind

proactive regional standards significantly. This mismatch remains a fundamental challenge for durable, long-term law application (Sadat et al., 2025).

Resource disparities across Pakistan's provinces also complicate consistent nationwide law application. Enforcement capacity varies significantly between urban centers and less-developed regional areas. Companies operating in smaller cities may face weaker regulatory oversight infrastructure locally. This creates inconsistent application depending purely on geographic business location. National-level policy coordination becomes essential for achieving consistent enforcement across all regions. Without strong coordination, ransom ware protections may effectively exist only in major cities. This regional disparity mirrors broader challenges already documented within Pakistan's legal framework. Addressing it requires deliberate resource allocation toward historically underserved regional enforcement units. Training programs would also need broader geographic reach beyond major urban centers. This challenge extends beyond cyber security law into wider systemic governance issues nationally. Board-level risk management perspectives confirm this uneven institutional capacity as an ongoing barrier (Pitafi, 2024).

Integrating new board-level accountability requirements into existing corporate governance also presents challenges. Many company boards currently lack cyber security expertise needed for meaningful oversight roles. Simply mandating board accountability does not automatically create genuine technical understanding. Companies may need mandatory training programs to build adequate boardroom cyber security literacy. This training requirement adds implementation cost and complexity for many organizations nationally. Smaller companies may particularly struggle to afford specialized board training programs quickly. Regulatory bodies would also need capacity to verify genuine compliance, not superficial documentation. Without proper verification mechanisms, board accountability requirements risk becoming purely symbolic exercises. Building genuine organizational resilience requires more than simply adding new legal requirements. It requires sustained cultural and educational investment across corporate governance structures broadly. Evidence linking internal auditing to cyber security outcomes supports this governance-integration argument directly (Al-Taie et al., 2025).

D. Practical Recommendations for Effective Legal Implementation

Pakistan should establish a specialized cybercrime regulatory body focused solely on corporate compliance. This body would oversee mandatory reporting, verify compliance, and coordinate enforcement nationally. Creating dedicated institutional capacity avoids overburdening existing agencies with unfamiliar technical responsibilities. This body should include cyber security experts, not only legal or policing personnel. International standards increasingly emphasize specialized institutions for effective corporate cyber security oversight globally. Pakistan can adapt these global standards while addressing local enforcement and resource limitations. This specialized body would also handle cross-border coordination for international ransom ware investigations. It could develop clear technical guidelines companies can follow for compliance purposes. Without dedicated institutional capacity, new legal provisions risk becoming difficult to enforce practically. Establishing this body should be an early implementation priority for policymakers. It creates the foundation needed for all other recommended reforms to function. This institutional approach reflects global trends in categorizing and structuring emerging cyber security regulation (Marotta & Madnick, 2025).

Phased implementation timelines would help companies adjust to new compliance requirements gradually. Large corporations could face immediate compliance deadlines given their greater available resources. Smaller businesses could receive extended timelines paired with targeted government compliance support. This phased approach prevents smaller firms from facing sudden, overwhelming regulatory burdens. It also allows regulators to refine enforcement processes before full nationwide rollout. Pilot programs in major financial and telecommunications sectors could test implementation first. Lessons learned from these pilots could then inform broader nationwide application later. This mirrors successful phased approaches seen in other national cyber security policy areas. Policymakers should intersect this phased rollout with existing national cyber security policy frameworks directly. Coordination prevents overlapping or contradictory compliance requirements across different regulatory bodies. This integrated approach ensures corporate compliance aligns with broader national security objectives. Phased implementation ultimately improves long-term compliance quality over rushed nationwide enforcement (Mirza, 2022).

Legal clarity must accompany implementation to avoid the ambiguity seen in earlier provisions. Historical analysis shows unclear legal language previously created inconsistent corporate liability outcomes. New provisions should define ransom ware, incident reporting, and compliance timelines with precision. Precise definitions reduce judicial interpretation burden and improve enforcement consistency across cases. Lawmakers should consult cyber

security practitioners when drafting technical definitions within legal text. This collaboration ensures legal language remains both enforceable and technically accurate simultaneously. Early PECA provisions suffered from gaps precisely because technical and legal expertise remained separate. Avoiding this mistake requires sustained collaboration throughout the entire drafting process. Public consultation periods could also help identify ambiguous language before final legislative passage. This transparent drafting process builds broader stakeholder trust in new compliance requirements. Learning from historical enactment challenges strengthens the durability of new legal provisions. Clear, precise language remains foundational to successful long-term law implementation (Zia Ul Islam et al., 2019).

Existing legal ambiguities within current provisions should be resolved before adding new obligations. Recent analysis highlights how unclear language can inadvertently affect fundamental corporate rights. Reformers should audit existing PECA sections for similar ambiguity before finalizing new amendments. This audit prevents new corporate obligations from inheriting old, unresolved legal problems. Legal drafters should specifically clarify how new reporting obligations affect data privacy protections. Companies need certainty that compliance will not create unintended legal exposure elsewhere. This clarity encourages good-faith compliance rather than defensive underreporting or excessive caution. Balancing corporate obligations with fundamental rights protections requires careful, deliberate legal drafting. Independent legal review panels could evaluate draft amendments before parliamentary approval processes begin. This additional review layer helps catch ambiguities before they become enforceable law. Addressing these ambiguities strengthens both corporate compliance and constitutional rights protections together. This careful approach reflects lessons directly drawn from recent legal ambiguity critiques (Haider & Hussain, 2026).

Institutional and policy failures identified in recent governance research must inform implementation strategy directly. Pakistan's cyber security governance has historically suffered from fragmented institutional responsibility and unclear authority. Implementation should therefore include clear delineation of regulatory authority across relevant government bodies. Overlapping jurisdiction between agencies has previously caused enforcement delays and inconsistent corporate treatment. New implementation plans should designate single-point regulatory authority for ransom ware compliance specifically. This reduces confusion for companies navigating multiple overlapping regulatory requirements simultaneously. Strategic reform recommendations emphasize building sustained institutional capacity rather than one-time legislative changes. Regular policy review cycles should assess whether implementation achieves intended corporate risk reduction. These reviews allow policymakers to adjust enforcement strategies based on real-world compliance outcomes. Comparative international case studies could also guide Pakistan's institutional reform choices effectively. Addressing these structural governance gaps remains essential for meaningful, lasting policy success. This approach directly incorporates strategic reform priorities identified within recent institutional analysis (Karim, 2026).

Implementation must also carefully balance corporate compliance obligations with broader digital rights concerns. Recent analysis warns that overly broad amendments risk enabling regulatory overreach beyond intended purposes. Policymakers should ensure new provisions target genuine ransom ware risk, not broader digital expression. Clear scope limitations should explicitly prevent misuse of reporting requirements for unrelated regulatory purposes. Independent oversight mechanisms could monitor whether enforcement remains within intended legislative boundaries consistently. This oversight builds public and corporate trust in the law's legitimate regulatory purpose. Transparent enforcement reporting could also demonstrate the law functions as originally intended. Regular public reporting on enforcement actions increases accountability and reduces overreach concerns significantly. This transparency directly addresses concerns raised in recent critical analysis of PECA amendments. Implementation success ultimately depends on maintaining this careful balance throughout enforcement practice. Achieving this balance ensures the law protects companies without compromising broader digital freedoms. This recommendation reflects direct lessons drawn from recent corporate compliance and oversight research (Aslam, 2025).

E. Implications of the Proposed Corporate Ransom Ware Reforms

This amendment would reshape how companies understand legal responsibility for ransom ware attacks. Boards would face direct accountability rather than treating cyber security as purely technical work. Current deterrence gaps have allowed companies to avoid meaningful legal consequences historically. Closing these gaps would likely increase corporate investment in preventive cyber security measures. Companies would need to budget specifically for compliance and risk management activities. This shift changes cyber security from a cost center into a governance priority. Legal accountability tends to influence corporate behavior more effectively than voluntary guidelines alone. Executives would need genuine understanding of ransom ware risks, not delegated technical awareness only. This

implication extends beyond individual companies into broader industry risk culture. Sectors handling sensitive data would likely see the strongest behavioral shifts first. Over time, this could reduce successful ransom ware attacks across regulated industries nationally. Strengthened deterrence provisions directly support this broader shift toward corporate accountability (Larena-Luengo et al., 2026).

Implementation would also expose existing structural weaknesses within Pakistan's enforcement institutions. Courts and investigative agencies would face increased caseloads involving complex corporate cyber security matters. This pressure could accelerate institutional reform that has been delayed for years. Without adequate preparation, enforcement backlogs may initially worsen before eventually improving. Agencies would need faster capacity building than typical bureaucratic timelines usually allow. This creates a genuine risk of uneven enforcement during the initial implementation period. Companies in better-resourced regions might see faster regulatory response than others. This disparity could persist until enforcement capacity develops more evenly nationwide. Structural gaps identified in earlier legal analysis foreshadow these implementation implications directly. Addressing them requires sustained political commitment beyond simply passing new legislation. Institutional strengthening remains a necessary companion to any new legal framework introduced. These implications highlight why enforcement capacity matters as much as legal text (Allahrakha, 2023)

Broader political implications also deserve careful consideration during implementation planning. Recent critical analysis warns that digital crime laws can sometimes enable authoritarian overreach. Expanding regulatory power always carries risk of misuse beyond original legislative intent. Policymakers must ensure new corporate provisions remain narrowly focused on ransom ware risk specifically. Broad or vague enforcement powers could otherwise chill legitimate corporate digital activity unintentionally. This risk requires careful legislative drafting and consistent independent judicial oversight afterward. Transparency in enforcement decisions would help prevent misuse of expanded regulatory authority. Civil society and legal scholars should continue monitoring implementation for signs of overreach. This ongoing scrutiny protects both corporate interests and broader digital rights simultaneously. Recent critiques of related legislative amendments highlight why this vigilance remains genuinely necessary. Balancing security objectives with rights protection remains an ongoing implementation challenge throughout enforcement. This tension will likely shape political debate around the amendment for years (Kumar, 2026).

Mandatory reporting requirements would directly affect how companies detect and respond to incidents. Research shows reporting mechanisms significantly influence whether cyber incidents get properly documented. Companies with clear reporting channels tend to identify and address threats faster. This implies mandatory reporting could improve corporate incident response quality nationally. Better documentation also creates valuable data for understanding national ransom ware attack patterns. Regulators could use this data to identify emerging threats affecting specific industries. This proactive intelligence gathering represents a significant improvement over current reactive approaches. Companies might also benefit from anonym zed threat intelligence shared back by regulators. This creates a feedback loop strengthening collective corporate cyber security resilience over time. Mediating factors identified in reporting mechanism research support this positive implementation pathway. Success depends heavily on companies trusting the reporting process genuinely protects their interests. This trust-building represents a critical implication for achieving meaningful compliance outcomes (Bhatti & Jamil, 2023).

International comparative analysis suggests Pakistan's reforms align with broader global legislative trends. Many jurisdictions have similarly moved toward mandatory ransom ware reporting and corporate accountability. This alignment could improve Pakistan's international standing in cyber security governance discussions. It may also facilitate better cross-border cooperation with international law enforcement agencies. Companies operating internationally would benefit from more consistent global compliance expectations. This reduces complexity for multinational corporations navigating different national legal requirements. Global legal analysis suggests successful implementations typically pair strong laws with adequate resources. Pakistan's success will likely depend on similarly matching legislative ambition with practical resources. Comparative insights from other jurisdictions could help Pakistan avoid common implementation mistakes. Learning from international experience remains a valuable implication for shaping Pakistan's specific approach. This global context suggests the amendment addresses a genuinely universal, evolving legal challenge. International alignment ultimately strengthens Pakistan's broader digital economy competitiveness over time (Worsley et al., 2025).

This amendment would influence how companies approach broader cyber threat mitigation strategies. Current mitigation approaches often focus narrowly on technical security measures alone. Legal accountability would encourage companies to adopt more comprehensive, governance-integrated mitigation strategies. This includes

combining technical defenses with clear organizational policies and employee training programs. Companies would need documented mitigation strategies demonstrating genuine, proactive risk management efforts. This shift moves cyber security from isolated IT departments into broader organizational strategy discussions. Existing research on Pakistan's cyber law framework supports strengthening these mitigation-focused corporate obligations. Advanced threats like ransom ware require this more holistic, organization-wide mitigation approach specifically. Companies adopting comprehensive strategies would likely experience fewer successful attacks over time. This implication extends benefits beyond individual companies into broader national cyber security resilience. Strengthened mitigation practices directly support the amendment's core corporate risk management objectives. This holistic approach represents a meaningful evolution in Pakistan's cyber law strategy (Awan et al., 2019).

CONCLUSION

Ransom ware has moved far beyond individual crime into a defining corporate governance challenge. This research examined how legal systems should reclassify ransom ware as formal corporate risk. It explored fiduciary duty, board accountability, and mandatory incident reporting across jurisdictions. Pakistan's Prevention of Electronic Crimes Act, 2016 illustrates this global legal gap clearly. The law originally targeted individual offenders, not systemic organizational vulnerabilities. Findings showed ransom ware now threatens business continuity, investor trust, and national economic stability together. Courts increasingly examine whether boards ignored foreseeable, preventable cyber security warning signs. This shift reflects a maturing legal theory connecting governance failure to genuine liability. Companies can no longer treat ransom ware as a purely technical problem for engineers. Boards must instead treat it as a core governance and risk responsibility. This reframing carries real consequences for how businesses operate in a connected world. Digital threats now sit squarely within corporate law, not outside it entirely.

Three connected arguments emerged throughout this study's examination of ransom ware and corporate accountability. First, existing legal frameworks struggle to define ransom ware within traditional cybercrime categories adequately. Second, mandatory reporting requirements would improve data quality and strengthen national policy responses significantly. Third, board-level accountability remains essential for shifting cyber security from reactive to preventive practice. These arguments connect through a shared theme of institutional and legal modernization. Weak definitions weaken enforcement, weak reporting weakens data, and weak accountability weakens prevention. Together, these gaps explain why ransom ware continues causing widespread, preventable corporate harm. Addressing one gap alone would not resolve the broader systemic problem identified here. Real progress requires coordinated reform across legal definitions, reporting duties, and governance standards. This connected approach strengthens the case for comprehensive, rather than piecemeal, legal reform. Recent global legislative trends increasingly support this integrated reform direction across many countries. Pakistan's amendment proposal reflects this same coordinated, multi-layered reform philosophy directly.

These findings carry meaningful implications for regulators, corporate boards, and legal practitioners worldwide. Clearer liability standards would help courts evaluate corporate conduct more consistently across cases. Mandatory reporting would give policymakers better tools for understanding evolving ransom ware attack patterns. Companies adopting proactive governance practices would likely reduce both financial and reputational damage. These findings apply directly to Pakistan's ongoing legislative discussions around PECA amendments. They also offer useful guidance for other developing economies facing similar governance gaps. Future research should examine how courts apply these standards once amendments take effect. Comparative studies across multiple developing nations could further strengthen this legal framework. Researchers might also explore how artificial intelligence complicates ransom ware detection and legal response. These unanswered questions point toward a growing, urgent area for continued legal scholarship. As digital threats keep evolving, corporate law must continue adapting alongside them steadily.

BIBLIOGRAPHY

Abdin, A. Z. U. (2025). Filling the gaps in Pakistan's national cyber security framework: A case for a comprehensive cybersecurity act in Pakistan. *Research Journal of Social Sciences and Arts, 4*(3). https://doi.org/10.71317/RJSA.004.03.1108

Ahmad, M. T. (2026). The Prevention of Electronic Crimes Act, 2016: Balancing cybercrime control and freedom of online expression in Pakistan. *Pakistan Journal of Humanities and Social Sciences, 14*(1). https://doi.org/10.52131/pjhss.2026.v14i1.3209

Al-Taie, B. F. K., Ali, S. I., & Al-Fandawi, H. H. F. (2025). The impact of corporate governance on cybersecurity risks: Internal auditing as a mediating variable. *International Journal of Business and Technology, 13*(3). https://doi.org/10.58915/ijbt.v13i3.297

Allahrakha, N. (2023). Balancing cyber-security and privacy: Legal and ethical considerations in the digital age. *Legal Issues in the Digital Age, 4*(2), 78–121. https://doi.org/10.17323/2713-2749.2023.2.78.121

Allahrakha, N. (2024). Who governs cyberspace in the age of AI? *Open Science Framework*. https://doi.org/10.31219/osf.io/6a2db

Aslam, M. A. (2025). Regulating misinformation or silencing dissent? A critical analysis of PECA amendments and corporate digital compliance in Pakistan. *Journal of Media and Communication Studies, 7*(2), 45–62. https://doi.org/10.59075/crsss

Awan, J. H., Memon, S., & Burfat, F. M. (2019). Role of cyber law and mitigation strategies in perspective of Pakistan to cope cyber threats. *International Journal of Cyber Warfare and Terrorism, 9*(2), 29–38. https://doi.org/10.4018/IJCWT.2019040103

Baker, T., & Shortland, A. (2023). The government behind insurance governance: Lessons for ransomware. *Regulation & Governance, 17*(4), 1000–1020. https://doi.org/10.1111/rego.12505

Baloch, A., & Abid, D. A. (2026). Cybercrime regulation in Pakistan: An assessment of the Prevention of Electronic Crimes Act, 2016 and the role of law enforcement agencies. *Social Science Review Archives, 4*(2), 1–18. https://doi.org/10.70670/sra.v4i2.2387

Bhatti, M. A., & Jamil, S. (2023). Factors effecting cyber incident occurrence: Mediating role of cyber incident reporting mechanism. *International Journal of Cyber Criminology, 17*(2), 112–133. https://doi.org/10.5281/zenodo.4766708

Bhutta, T. A., & Rashid, A. (2026). Cybersecurity governance in Pakistan: Evaluating public sector preparedness through International Telecommunication Union Global Cybersecurity Index framework. *Journal of Public Policy Practitioners, 5*(1), 1–25. https://doi.org/10.32350/jppp.51.03

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice, 47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: The moderating role of corporate governance in the MENA region. *Future Business Journal, 10*(1), Article 115. https://doi.org/10.1186/s43093-024-00402-9

Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2021). Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework. *Journal of Accounting and Public Policy, 40*(5), Article 106860. https://doi.org/10.1016/j.jaccpubpol.2021.106860

Gale, M., Bongiovanni, I., & Slapničar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security, 121*, Article 102840. https://doi.org/10.1016/j.cose.2022.102840

Haider, M. S., & Hussain, R. (2026). Legal ambiguity in Section 21 of PECA 2016 and its impact on fundamental rights in Pakistan: An analysis through legal language. *The Critical Review of Social Sciences Studies, 3*(1), 1–15. https://doi.org/10.59075/v01f4q50

Hansel, M. (2024). Ransomware as a threat to peace and security. *Journal of Cyber Policy, 9*(2), 245–268. https://doi.org/10.1080/23738871.2024.2357092

Iqbal, M. (2023). The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the challenges in Pakistan. *Siazga Research Journal, 2*(4), 273–282. https://doi.org/10.58341/srj.v2i4.35

Karim, A. (2026). Cybersecurity governance in Pakistan: Institutional gaps, policy failures, and strategic reforms. In *Digital transformation and cybersecurity in emerging economies* (pp. 185–210). Springer. https://doi.org/10.1007/978-3-032-28051-0_10

Kausar, S., & Laghari, A. R. (2025). Social engineering attacks in Pakistan: Analyzing the weakest link in cyber security. *Journal of Development and Social Sciences, 6*(1), 364–374. https://doi.org/10.47205/jdss.2025(6-I)32

Khadam, N. (2023). How to punish cyber criminals: A study to investigate the target and methods of cybercrimes in Pakistan. *Heliyon, 9*(12), Article e22634. https://doi.org/10.1016/j.heliyon.2023.e22634

Khan, A. U. A. (2025). Cyber crime in Pakistan: Trends, challenges, and legal responses. *Advance Social Science Archive, 4*(1), 1358–1366. https://doi.org/10.55966/assaj.2025.4.1.080

Khawaldeh, A. M. (2026). Civil liability odds in information leaks: Controversial legal debates and emerging judicial doctrines in Jordan. *Laws, 15*(2), Article 26. https://doi.org/10.3390/laws15020026

Kumar, R. (2026). Under the guillotine of digital authoritarianism: A critical review of Pakistan's Prevention of Electronic Crimes (Amendment) Act 2025. *SSRN Electronic Journal*. Advance online publication. https://doi.org/10.2139/ssrn.6965419

Larena-Luengo, A., Martínez-Herraiz, J.-J., Ferrer-Oliva, M., & Medina-Merodio, J.-A. (2026). Influence of human and organizational factors on security perception: Mediating role of cyber incident reporting mechanism. *International Journal of Information Security, 25*(3). https://doi.org/10.1007/s10207-026-01277-3

Liu, C., & Babar, M. A. (2026). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management, 51*(1), 62–92. https://doi.org/10.1177/03128962241293658

Lodhi, A. R. K., Sajjad, A., Akbar, K., Uddin, S. S., Jabeen, R., & Lashari, A. H. (2024). Artificial intelligence, cyber law, and data protection: Legal challenges and regulatory responses in the digital age. *TPM: Testing, Psychometrics, Methodology in Applied Psychology, 31*(2), 1–15. https://doi.org/10.4473/TPM31.2.1

Majeed, Y., Majeed, A., & Minhas, M. T. (2026). Cybersecurity governance in the digital era and IT: Integrating regulatory oversight, risk management, and organisational resilience. *Social Science Review Archives, 4*(1), 1–18. https://doi.org/10.70670/sra.v4i1.1711

Marotta, A., & Madnick, S. (2025). Analyzing and categorizing emerging cybersecurity regulations. *ACM Computing Surveys, 58*(2), 1–36. https://doi.org/10.1145/3757318

Mirza, M. N. (2022). 3-Cs of cyberspace and Pakistan: Cyber crime, cyber security, and cyber law. *Journal of Political Studies, 29*(S-I), 76–85. https://doi.org/10.47205/jps.2022(29-S-I)76

Opitz, E. L. (2018). Cybersecurity for the board of directors of small and midsized businesses. *Board Leadership, 2018*(159), 4–5. https://doi.org/10.1002/bl.30115

Pitafi, Z. R. (2024). Perspective chapter: Cybersecurity and risk management. In *Cybersecurity and risk management*. IntechOpen. https://doi.org/10.5772/intechopen.1186435

Sadat, A., Lawelai, H., & Younus, M. (2025). Comparative analysis of National Cyber Security Index: A case study of Pakistan and Indonesia. *Kasetsart Journal of Social Sciences, 46*(1), 1–12. https://doi.org/10.34044/j.kjss.2025.46.1.01

Saleem, H., Jan, J., & Areej, A. (2022). Cyber crimes trends in Pakistan: Analyzing the legal framework and enforcement challenges. *Society, Law and Policy Review, 1*(1), 10–22. https://doi.org/10.62585/slpr.v1i1.21

Shabana, S., & Rahman, A. (2024). Cyber crimes and security challenges in Pakistan: An analysis of PECA 2016 application. *Journal of Political Stability Archive, 4*(2), 16–28. https://doi.org/10.63468/jpsa.4.2.16

Sharma, D., Reddy, S., & Shahid, H. (2023). Cybersecurity obligations for critical infrastructure: Emerging legal norms, enforcement gaps, and governance challenges. *Legal Studies in Digital Age, 2*(3), 49–63. https://doi.org/10.61838/kman.lsda.322

Teichmann, F., & Wittmann, C. (2022). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. *Journal of Financial Crime, 30*(6), 1491–1498. https://doi.org/10.1108/JFC-04-2022-0093

Worsley, M. K., Kendall-Morwick, J., & Houston, K. A. (2025). Change waits for no one: An examination of the legal response to ransomware attacks. *Criminal Justice Policy Review, 36*(6), 259–280. https://doi.org/10.1177/08874034251363431

Zia Ul Islam, Khan, M. A., & Zubair, M. (2019). Cybercrime and Pakistan. *Global Political Review, 4*(2), 12–19. https://doi.org/10.31703/gpr.2019(IV-II).02