IRSHAD

International Journal of Cyber Law

Legal Reclassification of Global Ransomware as Corporate Risk

Malgozata Stvol[1*] · **Mansoor Noor Cheema**[2] · **Malik Imtiaz Khokhar**[3] · **Shaheen Iqbal Gujjar**[4] · **Malik Faisal Younas**[5]

[1] University of Gdansk, Poland
[2] Lahore University of Management Sciences, Lahore
[3] Lahore University of Management Sciences, Lahore
[4] Lahore Leads University, Lahore
[5] Lahore Leads University, Lahore

* *gulasmz@gmail.com*

ABSTRACT

Ransomware attacks cause severe financial and reputational damage to global corporations annually. Legal systems classify ransomware primarily as criminal conduct, ignoring broader corporate governance failures. This research examines how legal reclassification could clarify director accountability and disclosure obligations. Current corporate law lacks clear standards addressing cybersecurity preparedness and fiduciary duty. Shareholders face limited remedies challenging inadequate board oversight following major ransomware incidents. Insurance markets struggle pricing risk without consistent legal liability standards across jurisdictions. This study analyzes existing legal frameworks, identifying significant gaps between criminal and corporate law. Findings reveal fragmented disclosure requirements, weak fiduciary recognition, and inconsistent regulatory enforcement globally. This research proposes reclassifying ransomware as formal corporate risk within governance frameworks. Such reclassification would strengthen director accountability, shareholder protection, and insurance market stability. The study offers practical recommendations for policymakers, courts, and corporate boards. This framework connects fragmented legal domains, addressing modern digital security challenges comprehensively and effectively.

Keywords: *Ransomware, Corporate Governance, Legal Reclassification, Fiduciary Duty, Cybersecurity Disclosure, Shareholder Protection, Director Accountability*

HOW TO CITE THIS ARTICLE (APA 7th Edition)

Stvol, M., Cheema, M. N., Khokhar, M. I., Gujjar., S. I., & Youns, M.F. (2026). Legal Reclassification of Global Ransomware as Corporate Risk. *International Journal of Cyber Law*, 1(1), 01–14. https://doi.org/10.59022/iijcl.003

I. INTRODUCTION

Ransomware attacks now strike a business every few seconds across the world. This threat has grown from a technical nuisance into a serious corporate danger. Companies lose millions of dollars from stolen data and halted operations. Legal systems still treat ransomware mainly as a criminal offense. This narrow view ignores the financial damage suffered by shareholders and employees. Courts and regulators must start viewing ransomware through a corporate risk lens. Such reclassification would push companies toward stronger cybersecurity governance and disclosure duties. Insurance markets would also benefit from clearer legal standards on ransomware liability. Directors could face real accountability for ignoring known cyber vulnerabilities. This shift connects criminal law with corporate governance and financial regulation. Small businesses often lack resources to survive a major ransomware attack. Large corporations also struggle despite having stronger cybersecurity budgets and legal teams. The following sections examine why this legal reclassification matters. They also explore how courts and lawmakers can achieve it (Rakha, 2022).

Ransomware has existed since the late 1980s as a minor cyber threat. Early attacks targeted individual computers and demanded small payments. Modern ransomware now targets hospitals, banks, and government agencies worldwide. Attackers use encryption to lock entire networks within minutes. Criminal law traditionally handles ransomware as theft or extortion. This approach focuses on punishing individual hackers after attacks occur. Corporate law rarely addresses ransomware as a business risk. Few scholars have studied ransomware through corporate governance frameworks. Most legal research treats cybercrime and corporate risk as separate fields. This separation creates confusion about who bears legal responsibility. Shareholders often lack legal remedies when ransomware damages company value. Directors face unclear duties regarding ransomware prevention and disclosure. Existing laws fail to connect criminal liability with corporate accountability. This gap leaves companies vulnerable and legal frameworks incomplete. This study bridges criminal law and corporate risk management (Jaffe et al., 2024).

Ransomware attacks now cause severe financial damage to global corporations. Legal systems classify these attacks primarily as criminal offenses against victims. This classification ignores the broader corporate consequences of ransomware incidents. Companies suffer lost revenue, damaged reputation, and legal liability after attacks. Current corporate law provides no clear framework for ransomware accountability. Directors face ambiguous duties regarding cybersecurity preparedness and incident disclosure. Shareholders cannot easily hold boards responsible for inadequate ransomware protection. Insurance markets struggle without consistent legal standards for ransomware liability. Regulators lack unified guidance connecting cybercrime with corporate governance failures. This research addresses the absence of ransomware as corporate risk. It examines how legal reclassification could clarify director responsibilities. It also explores how disclosure duties might reduce shareholder harm. The study identifies specific gaps between criminal law and corporate regulation. It proposes solutions connecting these separate legal domains effectively. This reclassification could strengthen corporate governance against ransomware threats (Vidović et al., 2025).

Recent studies show ransomware attacks increased sharply between 2020 and 2025. Researchers found healthcare and financial sectors face the highest attack rates. Scholars identified weak cybersecurity governance as a major corporate vulnerability. Legal experts noted inconsistent disclosure requirements across different jurisdictions worldwide. Studies revealed directors often lack clear cybersecurity oversight responsibilities. Corporate governance researchers linked poor board preparedness to ransomware damage severity. Analysts found insurance companies struggle pricing ransomware risk accurately. Legal scholars observed criminal law frameworks ignore corporate accountability gaps. Researchers highlighted shareholder lawsuits following ransomware incidents remain rare globally. Studies from 2022 showed regulatory guidance varies significantly between countries. Cybersecurity researchers documented rising ransom payments despite law enforcement warnings. Legal analysts noted courts rarely address ransomware within corporate law disputes. Scholars called for unified frameworks connecting cybercrime and governance failures. These findings collectively reveal significant academic and regulatory gaps (Bello et al., 2025).

Additional research from 2021 examined mandatory disclosure laws for ransomware incidents. Findings showed disclosure requirements often lack enforcement mechanisms globally. Scholars studying European Union regulations found stronger corporate accountability standards emerging. Comparative legal studies revealed United States frameworks remain fragmented across states. Researchers analyzing 2023 data found ransomware costs exceeding billion annually worldwide. Legal scholars proposed treating ransomware preparedness as a fiduciary duty. Studies on corporate boards found few directors received cybersecurity training. Analysts noted small businesses face disproportionate ransomware damage compared to large firms. Recent scholarship suggested integrating cybersecurity metrics into corporate risk disclosures. Legal researchers found existing case law provides limited guidance for courts.

Studies published in 2025 emphasized cross-border enforcement challenges for ransomware crimes. Scholars argued current frameworks fail protecting shareholder interests adequately. These gaps demonstrate the need for reclassifying ransomware as corporate risk. This research directly addresses these identified academic and legal shortcomings (Cremer et al., 2022).

Existing literature identifies ransomware as both a criminal and financial threat. However, few studies connect ransomware directly to corporate governance obligations. Most research treats cybersecurity and corporate law as separate legal areas. This separation leaves directors without clear guidance on ransomware accountability. Scholars have examined disclosure laws but rarely proposed unified reclassification frameworks. Comparative studies highlight regulatory differences but lack concrete legal solutions. Few researchers have analyzed ransomware through a fiduciary duty lens. Insurance and risk management studies remain disconnected from corporate governance research. This gap prevents courts from developing consistent ransomware liability standards. Existing frameworks fail addressing shareholder protection during major cyber incidents. Future research must integrate criminal law with corporate risk classification. This study fills that gap through legal reclassification analysis. It proposes treating ransomware preparedness as a core governance duty. This approach connects fragmented legal fields into a unified framework (Phipps et al., 2025).

To examine the legal gaps that prevent courts from treating ransomware as a corporate governance risk.

To analyze how legal reclassification of ransomware could clarify director duties and accountability standards.

To propose a unified legal framework connecting criminal liability, corporate governance, and disclosure obligations for ransomware incidents.

How can the legal reclassification of ransomware as a corporate governance risk clarify director accountability and strengthen disclosure obligations under existing corporate law frameworks?

This research holds significant value for legal scholars and corporate practitioners. It bridges a critical gap between criminal law and corporate governance. Directors and boards will gain clearer guidance on cybersecurity accountability. Courts will benefit from a structured framework for ransomware liability cases. Shareholders will find stronger legal grounds for protecting their financial interests. Insurance companies will gain clearer standards for pricing ransomware risk accurately. Regulators can use this framework to design consistent disclosure requirements. Policymakers will find practical recommendations for updating outdated legal frameworks. This study contributes new knowledge connecting cybercrime with corporate risk management. It offers a fresh legal perspective absent from current academic literature. Practitioners advising corporate clients will benefit from clearer risk classification standards. Legal educators can use this research to teach emerging cyber law topics. This work ultimately strengthens corporate resilience against growing ransomware threats. It provides a foundation for future research connecting these legal domains (Khan et al., 2024).

II. METHODOLOGY

This research follows a qualitative research design suited for legal analysis. Qualitative methods allow deep examination of laws, regulations, and legal principles. This study focuses on doctrinal analysis examining existing corporate and criminal law frameworks. The population for this research includes global laws addressing ransomware and corporate governance. The sample includes specific regulations, corporate governance codes, and cybersecurity disclosure laws. This research analyzes laws related to corporate fiduciary duties and cybersecurity obligations. Relevant frameworks include corporate governance codes, cybersecurity disclosure regulations, and shareholder protection laws. Data collection relies on scholarly literature, legal statutes, and regulatory guidance documents. Specific keywords guided this search, including ransomware, corporate risk, and fiduciary duty. Additional keywords included cybersecurity governance, director accountability, and disclosure obligations. These keywords helped identify relevant scholarly articles, case law, and regulatory materials effectively.

This research retrieved legal materials directly from official government and regulatory websites. Scholarly articles were retrieved from established academic databases containing peer-reviewed legal research. This study prioritized recent publications, generally not exceeding five years old. Recent sources ensure this research reflects currently applicable laws and regulations. Materials were selected based on relevance to corporate governance and cybersecurity topics. Authors were evaluated based on academic credentials, institutional affiliation, and publication history. This research favored peer-reviewed articles published within recognized legal and academic journals. Sources were assessed based on citation frequency and use by other researchers. Official regulatory documents were treated as

primary sources carrying authoritative legal weight. This approach ensured the research maintained strong academic validity and reliability standards.

Data analysis relied primarily on doctrinal analysis examining statutes, regulations, and legal principles. This research also employed document analysis examining scholarly articles and policy papers. Doctrinal analysis helped identify gaps, inconsistencies, and contradictions within existing legal frameworks. This research maintained strict ethical standards throughout the entire research process. Only publicly available official documents and scholarly materials were used throughout. Every scholarly article referenced received proper citation acknowledging original authors and their contributions. This research maintained no conflicts of interest throughout the entire research process. The study addresses several important limitations affecting overall conclusions and generalizability. Ransomware technology continues evolving rapidly, creating challenges predicting long-term legal relevance. Corporate governance policies also change frequently, potentially affecting the applicability of specific findings. These limitations suggest conclusions should be understood within a specific evolving legal context. Delimitations include focusing specifically on corporate governance rather than broader criminal law issues.

III. RESULTS

This research examined how legal reclassification could address ransomware corporate risk. Seven distinct results emerged from analyzing current legal frameworks and gaps. These results directly answer the research question about director accountability standards. Each finding highlights specific weaknesses within existing corporate governance frameworks. The analysis reveals significant ambiguity surrounding director duties for cybersecurity preparedness. It also exposes inconsistent disclosure requirements across different legal jurisdictions worldwide. Furthermore, the findings demonstrate fragmentation between criminal law and corporate governance. Shareholders currently lack effective remedies for challenging inadequate cybersecurity oversight decisions. Insurance markets face uncertainty due to unclear corporate liability standards. Courts rarely recognize cybersecurity preparedness as part of fiduciary duty obligations. Regulatory gaps also hinder cross-border enforcement of corporate cybersecurity accountability. These results collectively support reclassifying ransomware as a formal corporate risk. This reclassification would strengthen governance, disclosure, and shareholder protection mechanisms. The following results present detailed findings addressing these identified legal gaps (Rakha, 2023).

Corporate law traditionally focuses on financial mismanagement and fiduciary breaches. Cybersecurity threats like ransomware remain largely absent from these frameworks. Directors face no clear legal standard for cybersecurity preparedness duties. Courts rarely hold boards accountable for inadequate ransomware prevention measures. This ambiguity creates confusion about acceptable levels of cyber risk management. Companies suffer significant losses while directors avoid meaningful legal consequences. Shareholders find limited legal pathways for challenging poor cybersecurity oversight. Existing fiduciary duty standards fail addressing modern digital security threats adequately. Boards often delegate cybersecurity decisions without establishing clear governance structures. This delegation creates gaps in accountability when ransomware attacks succeed. Legal scholars argue directors need explicit cybersecurity oversight obligations established. Courts require clearer benchmarks for evaluating director cybersecurity decision-making processes. Without these standards, accountability remains inconsistent across different corporate structures. Legal reclassification would establish concrete director duties regarding ransomware preparedness. This clarity would strengthen corporate governance and protect shareholder interests effectively (Teichmann et al., 2022).

Different countries maintain separate legal standards for ransomware incident disclosure. The European Union requires strict reporting timelines under specific regulatory frameworks. The United States lacks unified federal requirements across different states. This inconsistency creates significant compliance challenges for multinational corporations operating globally. Companies often struggle determining which disclosure standard applies to specific incidents. Some jurisdictions require immediate public disclosure after ransomware attacks occur. Other jurisdictions permit delayed reporting until investigations reach specific conclusions. This variation undermines investor confidence in corporate cybersecurity risk management practices. Shareholders receive inconsistent information depending on company headquarters location. Regulators struggle enforcing standards across borders without harmonized legal frameworks. This fragmentation allows companies to exploit weaker disclosure jurisdictions strategically. Legal reclassification could establish baseline international disclosure standards for ransomware. Such standards would ensure consistent shareholder protection regardless of jurisdiction. This approach would strengthen global corporate accountability for cybersecurity incidents significantly (Umeanozie et al., 2025).

Criminal law treats ransomware primarily as theft or extortion offenses. This framework focuses narrowly on punishing individual hackers after attacks occur. Corporate law separately governs director duties and organizational risk management practices. These two legal domains rarely intersect within current judicial interpretations. Courts prosecute ransomware perpetrators without examining corporate governance failures simultaneously. This separation prevents comprehensive accountability for both criminals and negligent boards. Companies avoid legal consequences despite inadequate cybersecurity preparedness before attacks. Prosecutors focus resources on catching hackers rather than corporate negligence. Civil courts rarely connect criminal ransomware incidents to corporate governance breaches. This fragmentation leaves victims without complete legal recourse against negligent companies. Legal scholars argue these domains require formal integration through statutory reform. Combining criminal and corporate law would create comprehensive accountability frameworks. Such integration would address both perpetrators and enabling corporate negligence. This research proposes bridging these fragmented legal domains through reclassification. This approach would strengthen overall legal responses to ransomware threats (Simanjuntak et al., 2025).

Shareholders invest significant capital trusting boards with sound governance decisions. Ransomware attacks often reveal serious weaknesses in corporate cybersecurity preparedness. Current legal frameworks provide shareholders limited tools for challenging these failures. Derivative lawsuits require proving specific breaches of established fiduciary duties clearly. Courts rarely recognize cybersecurity negligence as a fiduciary duty breach. This reluctance leaves shareholders without meaningful legal recourse after major attacks. Companies lose substantial market value while boards avoid direct legal consequences. Shareholders bear financial losses without corresponding accountability from negligent directors. Legal standards fail connecting cybersecurity preparedness to traditional governance duty frameworks. This gap discourages boards from prioritizing adequate ransomware prevention investments. Stronger legal remedies would incentivize proactive cybersecurity governance among corporate boards. Reclassifying ransomware as corporate risk would strengthen shareholder protection mechanisms significantly. Courts could then evaluate cybersecurity decisions using established fiduciary duty standards. This approach would create meaningful accountability for inadequate governance practices. Shareholders would gain stronger legal grounds for challenging future cybersecurity negligence (Ashraf et al., 2023).

Insurance companies offer cyber liability coverage without consistent legal risk benchmarks. Ransomware liability standards remain unclear across different corporate legal jurisdictions. This uncertainty makes accurate risk pricing extremely difficult for insurers globally. Companies purchase coverage without knowing their actual legal exposure levels. Insurers struggle setting premiums that reflect true corporate cybersecurity risk profiles. Some insurers have withdrawn from ransomware coverage due to unpredictable claims. This withdrawal leaves companies vulnerable without adequate financial protection options. Claims disputes frequently arise from ambiguous corporate liability determinations after attacks. Courts provide inconsistent rulings on insurer obligations following ransomware incidents. This inconsistency increases litigation costs for both insurers and policyholders significantly. Clearer legal liability standards would stabilize the cyber insurance market considerably. Insurers could then price policies based on established corporate risk classifications. Companies would gain predictable coverage terms reflecting genuine legal exposure levels. Legal reclassification directly addresses this market uncertainty through defined risk standards. This clarity would benefit insurers, companies, and shareholders collectively (Tsohou et al., 2023).

IV. DISCUSSION

A. Legal Ambiguity in Director Accountability

This finding shows corporate law has not kept pace with growing cyber threats. Directors face ransomware risks without any clear legal roadmap for action. Traditional fiduciary duty standards focus on financial decisions and business judgment. These standards rarely extend explicitly into digital security and cyber preparedness. This gap creates real confusion for boards trying to manage cyber risk. Companies invest inconsistently in cybersecurity because legal expectations remain undefined. Some boards prioritize compliance minimums rather than genuine risk reduction efforts. This ambiguity ultimately weakens corporate resilience against increasingly sophisticated ransomware attacks. Recent high-profile attacks on hospitals and pipelines highlight this governance weakness. Lawmakers have started discussing stronger cybersecurity requirements for corporate boards. However, formal legal standards have not yet emerged from these discussions (Hayes, 2026).

This ambiguity carries serious practical consequences for companies and their stakeholders. Without clear duties, directors cannot be held meaningfully accountable for negligence. Shareholders lose money while boards

escape legal responsibility for poor preparation. Employees and customers also suffer when companies fail preventing preventable attacks. This weak accountability structure discourages boards from prioritizing cybersecurity investment seriously. Companies often treat cybersecurity as a technical issue, not a governance duty. This mindset persists because courts rarely challenge board decisions on cyber matters. The absence of legal consequences removes incentives for proactive risk management. Stronger accountability standards could shift this mindset toward genuine governance responsibility. Boards would then treat cybersecurity as central to their fiduciary obligations. This shift could meaningfully reduce ransomware damage across affected industries.

Several examples support the argument that legal ambiguity harms corporate accountability. Major ransomware attacks on critical infrastructure revealed weak board oversight repeatedly. Investigations often found companies ignored known vulnerabilities before attacks occurred. Despite this negligence, few directors faced formal legal consequences afterward. Regulatory bodies issued warnings but lacked authority enforcing meaningful accountability measures. This pattern repeats across industries, showing systemic rather than isolated governance failures. Financial regulators have begun proposing stricter cybersecurity disclosure and preparedness rules. These proposals suggest growing recognition that current standards remain insufficient. However, implementation across jurisdictions remains slow and inconsistent globally. This evidence strengthens the argument for formal legal reclassification of ransomware. Clear standards would provide courts concrete benchmarks for evaluating director conduct.

This analysis carries certain limitations worth acknowledging honestly. Legal ambiguity varies across jurisdictions, making universal conclusions somewhat difficult. Some countries have stronger cybersecurity governance expectations than others currently. This research focuses primarily on gaps rather than measuring their exact financial impact. Available data on boardroom cybersecurity decisions often remains confidential or unavailable. This limits researchers' ability to fully assess director decision-making processes. Additionally, ransomware tactics evolve quickly, potentially outpacing legal reform efforts. Standards created today might require frequent updates as threats change. Company size and industry also influence how ambiguity affects different boards. Large corporations often have more resources addressing cybersecurity than smaller companies. These variations suggest reclassification efforts must remain flexible and adaptable.

Comparing different legal systems reveals interesting contradictions worth examining closely. Some jurisdictions have introduced stricter cybersecurity governance requirements for corporate boards. Other regions maintain traditional fiduciary duty standards without cybersecurity-specific provisions. This inconsistency creates competitive disadvantages for companies operating within stricter frameworks. Meanwhile, companies in weaker jurisdictions face fewer legal pressures toward preparedness. This contradiction undermines arguments that market forces alone will drive improvement. Companies without legal pressure often underinvest in cybersecurity despite genuine risks. This pattern contradicts assumptions that reputational risk alone motivates adequate preparation. These contradictions suggest voluntary measures remain insufficient without formal legal requirements. Consistent global standards would reduce these competitive and regulatory disparities significantly. This comparison strengthens the case for coordinated international legal reform efforts.

These findings carry significant implications for lawmakers, regulators, and corporate boards. Clearer director duties would provide meaningful accountability following ransomware incidents. This accountability could shift corporate culture toward proactive cybersecurity investment strategies. Regulators could use clarified standards for enforcing consistent disclosure requirements globally. Insurance markets would benefit from clearer risk classifications for pricing purposes. Legal reclassification offers practical applicability across multiple stakeholder groups simultaneously. Corporate boards would gain concrete guidance for structuring cybersecurity oversight responsibly. Shareholders would gain stronger legal tools for challenging inadequate governance decisions. Courts would gain consistent benchmarks for evaluating director conduct fairly. Policymakers should prioritize these reforms given rising global ransomware threats. This research provides a foundation for developing such practical legal frameworks (Gale et al., 2022).

B. Disclosure Inconsistency Across Jurisdictions

This finding reveals how fragmented global disclosure laws weaken corporate accountability. Companies operating across multiple countries face conflicting reporting timelines and standards. Some regions demand immediate public disclosure after ransomware attacks occur. Others allow companies significant delays before informing regulators or shareholders. This inconsistency creates strategic opportunities for companies avoiding transparent communication. Multinational corporations often choose jurisdictions offering weaker disclosure

requirements deliberately. This behavior undermines the broader goal of protecting investors and consumers. Recent policy discussions have emphasized harmonizing cybersecurity disclosure across borders. The European Union has moved toward stricter unified reporting frameworks recently. Other regions continue debating similar reforms without reaching clear consensus yet. This ongoing global inconsistency directly supports the case for legal reclassification (Liu et al., 2026).

This disclosure gap carries meaningful consequences for shareholders and financial markets. Investors cannot accurately assess corporate cybersecurity risk without consistent reporting standards. Delayed disclosure often means investors learn about attacks too late. This timing gap prevents shareholders from making informed investment decisions promptly. Weak disclosure requirements also reduce pressure on companies improving cybersecurity practices. Companies facing minimal reporting obligations often deprioritize preventive security investments. This pattern creates systemic risk across international financial markets and industries. Strong disclosure requirements would incentivize companies strengthening cybersecurity before incidents occur. Investors would gain better tools evaluating corporate risk management performance. This improved transparency could restore stronger investor confidence in affected markets. Consistent global standards remain essential for achieving these meaningful improvements.

Specific examples illustrate how disclosure inconsistency affects real corporate outcomes. Some companies delayed informing shareholders about major ransomware attacks for months. This delay allowed executives selling shares before public disclosure damaged stock prices. Regulators later criticized these companies but lacked strong enforcement authority initially. Similar incidents occurred across different jurisdictions with varying regulatory responses. Stronger jurisdictions imposed meaningful penalties while others issued only symbolic warnings. This disparity demonstrates how weak enforcement undermines broader disclosure policy goals. Recent regulatory proposals suggest stricter penalties for delayed ransomware incident reporting. These proposals reflect growing recognition that current enforcement remains genuinely inadequate. Consistent international standards would strengthen enforcement across all major jurisdictions equally. This evidence reinforces arguments supporting formal legal reclassification of ransomware risk.

This analysis acknowledges certain limitations regarding disclosure inconsistency across jurisdictions. Available data on delayed disclosures often remains incomplete or difficult accessing. Companies rarely publicize exact timelines between attack discovery and disclosure. This limits researchers' ability to measure disclosure delays precisely across cases. Additionally, cultural and political factors influence disclosure expectations differently across regions. Some countries prioritize corporate privacy over aggressive public disclosure requirements. These differing values complicate efforts creating universally accepted disclosure standards. Legal reforms must therefore balance transparency goals with legitimate privacy considerations carefully. Furthermore, rapidly evolving ransomware tactics complicate establishing fixed disclosure timelines effectively. Standards created today may require frequent revision as attack methods change. These limitations suggest reclassification efforts must remain adaptable and internationally coordinated.

Comparing disclosure frameworks across regions reveals significant contradictions worth noting. Stricter jurisdictions assume mandatory disclosure improves overall corporate cybersecurity behavior. However, some companies simply relocate operations avoiding stringent disclosure requirements entirely. This contradiction suggests strict rules alone cannot guarantee improved corporate behavior. Weaker jurisdictions assume market forces alone will encourage voluntary transparency efforts. Evidence shows companies rarely disclose voluntarily without meaningful legal requirements present. This contradiction challenges assumptions that reputation concerns sufficiently motivate corporate transparency. These conflicting approaches demonstrate why coordinated international standards remain genuinely necessary. Isolated national reforms cannot address inherently global and interconnected ransomware threats. This comparison strengthens arguments favoring unified legal reclassification across multiple jurisdictions.

These findings offer significant guidance for policymakers designing future disclosure regulations. Lawmakers should prioritize harmonizing disclosure timelines across major global jurisdictions. Consistent standards would reduce opportunities for companies exploiting regulatory differences strategically. Regulators could then enforce meaningful penalties for delayed or incomplete disclosures. Insurance companies would benefit from predictable disclosure patterns supporting accurate risk assessment. Shareholders would gain timely information supporting more informed investment decision-making processes. Corporate boards would gain clearer expectations guiding their disclosure practice decisions. This research demonstrates practical applicability for regulators, investors, and corporate governance professionals. Legal reclassification directly addresses these disclosure inconsistencies through unified

accountability frameworks. Policymakers should consider these findings when developing future international cybersecurity regulations (Tariq, 2025).

C. Fragmented Legal Frameworks Between Criminal and Corporate Law

This finding highlights a structural problem within existing legal systems. Criminal law and corporate law operate as separate, disconnected legal domains. Criminal courts prosecute hackers while ignoring underlying corporate governance failures entirely. Corporate courts address shareholder disputes without considering criminal cybersecurity context. This separation prevents comprehensive legal responses to complex ransomware incidents. Companies benefit from this fragmentation by avoiding accountability for negligent preparation. Prosecutors focus limited resources on catching individual criminal perpetrators exclusively. Meanwhile, corporate boards escape scrutiny despite enabling conditions allowing attacks succeeding. Recent policy discussions have called for integrated approaches connecting these domains. Some countries have begun exploring hybrid frameworks addressing both dimensions simultaneously. However, comprehensive legal integration remains rare across most global jurisdictions currently (Andre et al., 2024).

This fragmentation creates serious practical consequences for victims seeking complete justice. Companies suffer attacks partly caused by inadequate cybersecurity governance decisions beforehand. Yet legal systems rarely connect these governance failures to criminal incident outcomes. This disconnect allows negligent boards avoiding meaningful legal or financial consequences. Shareholders bear losses while responsible parties escape comprehensive legal accountability entirely. This pattern discourages boards from prioritizing genuine cybersecurity risk management investments. Companies calculate minimal legal risk from inadequate preparation under current fragmented frameworks. Integrated legal approaches would change this calculation significantly for corporate boards. Boards would then face accountability spanning both criminal and civil law dimensions. This integration could meaningfully improve corporate cybersecurity preparedness across affected industries. Stronger integrated frameworks would better serve justice for all stakeholders involved.

Specific cases demonstrate how legal fragmentation produces incomplete accountability outcomes. Major ransomware attacks resulted in criminal prosecutions targeting only individual hackers. Corporate boards enabling these attacks through negligence faced no parallel legal consequences. Investigations revealed known vulnerabilities that boards ignored before attacks occurred repeatedly. Despite this evidence, prosecutors lacked authority connecting criminal cases to corporate negligence. Civil courts separately handled shareholder lawsuits without referencing criminal investigation findings. This siloed approach prevented comprehensive understanding of complete incident circumstances. Some legal scholars have proposed creating specialized courts handling integrated cyber cases. These proposals suggest growing recognition that current fragmented approaches remain insufficient. Consistent frameworks connecting criminal and corporate law would strengthen overall accountability considerably.

This analysis acknowledges important limitations regarding legal framework fragmentation research. Measuring the exact impact of fragmentation requires comparing outcomes across many cases. Available data connecting criminal prosecutions to corporate governance decisions remains limited significantly. Court records often separate criminal and civil proceedings, complicating comprehensive analysis efforts. Additionally, legal traditions differ significantly between common law and civil law systems. These differences complicate creating universally applicable integrated legal frameworks globally. Furthermore, expanding legal frameworks connecting these domains carries potential unintended consequences. Overly broad integration might create excessive litigation or regulatory compliance burdens. These limitations suggest reform efforts must balance integration with practical implementation considerations carefully.

Comparing different legal traditions reveals notable contradictions worth examining carefully. Common law systems generally maintain stricter separation between criminal and civil proceedings. Civil law systems sometimes allow greater flexibility connecting these different legal dimensions. This difference creates inconsistent global approaches toward addressing ransomware accountability comprehensively. Some jurisdictions assume criminal prosecution alone sufficiently addresses ransomware related harms. Evidence suggests this assumption ignores significant corporate governance failures enabling attacks. This contradiction demonstrates why purely criminal approaches remain fundamentally incomplete solutions. Other jurisdictions assume civil remedies alone adequately address shareholder financial losses. This assumption similarly ignores necessary criminal accountability for direct attack perpetrators. These contradictions collectively support arguments favoring comprehensive integrated legal reform approaches.

These findings carry substantial implications for judicial systems and legal reformers. Lawmakers should consider developing frameworks connecting criminal and corporate law domains. Courts could benefit from specialized training addressing complex cyber governance cases. Prosecutors and civil litigators could coordinate more effectively addressing comprehensive incident circumstances. Regulators could design policies encouraging information sharing between criminal and civil proceedings. Corporate boards would face stronger incentives toward genuine cybersecurity preparedness investments. This integrated approach offers practical applicability across judicial, regulatory, and corporate contexts. Shareholders would benefit from more comprehensive accountability addressing complete incident circumstances. Policymakers should prioritize this integration given increasing ransomware complexity and frequency. This research provides meaningful groundwork supporting future comprehensive legal framework development (Irvita et al., 2025).

D. Limited Shareholder Remedies for Cyber Governance Failures

This finding exposes a significant weakness in shareholder protection mechanisms. Shareholders invest trusting boards will manage risks responsibly and diligently. Ransomware attacks frequently reveal inadequate cybersecurity governance decisions made beforehand. Current legal remedies rarely address these specific governance failures effectively. Derivative lawsuits require proving clear fiduciary duty breaches under strict standards. Courts have historically shown reluctance recognizing cybersecurity negligence as such breaches. This reluctance leaves shareholders without meaningful legal pathways following major attacks. Companies lose substantial value while responsible directors avoid genuine accountability entirely. Recent shareholder activism has pushed for stronger cybersecurity governance oversight demands. Some investors now demand cybersecurity expertise on corporate boards directly. However, formal legal remedies addressing these concerns remain largely undeveloped currently (Song et al., 2026).

This remedy gap produces serious consequences affecting shareholder financial interests directly. Shareholders absorb losses from preventable attacks without corresponding legal recourse available. This imbalance discourages boards from prioritizing adequate cybersecurity investment decisions seriously. Companies calculate minimal legal risk from inadequate preparation under current frameworks. Weak accountability structures create troubling incentives favoring cost-cutting over genuine security. This pattern ultimately increases systemic risk across entire industries and markets. Stronger shareholder remedies would incentivize boards prioritizing meaningful cybersecurity governance improvements. Boards would then face real financial consequences for demonstrated cybersecurity negligence. This shift could significantly reduce ransomware vulnerability across affected corporate sectors. Improved remedies would also restore greater investor confidence in corporate governance. This confidence remains essential for maintaining healthy and stable financial markets.

Several examples demonstrate how limited remedies produce troubling accountability gaps. Shareholders filed lawsuits following major ransomware attacks at large corporations. Courts frequently dismissed these cases, citing insufficient evidence of fiduciary breaches. Despite clear evidence of ignored warnings, boards avoided meaningful legal consequences. This pattern repeated across multiple high-profile ransomware incidents in recent years. Investors grew frustrated watching negligent boards escape accountability repeatedly and consistently. Some jurisdictions have begun exploring stronger governance liability standards for cybersecurity. These developments suggest growing recognition that current remedies remain genuinely inadequate. Legal reclassification would provide courts clearer standards for evaluating these claims. This clarity would strengthen shareholder positions when pursuing legitimate governance failure claims.

This analysis acknowledges certain limitations regarding shareholder remedy research conclusions. Measuring the full financial impact of governance failures requires extensive case analysis. Available data on dismissed shareholder lawsuits often lacks detailed reasoning explanations. This limits researchers' ability to fully understand judicial reluctance patterns. Additionally, shareholder remedy standards vary significantly across different legal jurisdictions globally. Some countries maintain stronger shareholder protection traditions than others currently do. These variations complicate creating universally applicable shareholder remedy frameworks effectively. Furthermore, expanding shareholder remedies carries potential unintended consequences worth careful consideration. Overly broad liability standards might discourage qualified individuals from serving as directors. These limitations suggest reform efforts must balance accountability with practical governance considerations.

Comparing shareholder remedy frameworks across jurisdictions reveals interesting contradictions worth noting. Some legal systems assume business judgment protections sufficiently shield reasonable board decisions. This assumption sometimes extends inappropriately to genuinely negligent cybersecurity preparation decisions. Other

systems maintain stricter standards holding directors accountable for foreseeable risks. This inconsistency creates uneven outcomes for similarly situated shareholders across jurisdictions. Some jurisdictions assume market discipline alone will punish poorly governed companies. Evidence suggests markets often fail punishing companies adequately following ransomware incidents. This contradiction challenges assumptions that market forces alone ensure accountability. These contradictions collectively support arguments favoring clearer statutory shareholder remedy standards.

These findings carry important implications for lawmakers and corporate governance reformers. Legislators should consider establishing clearer statutory standards for cybersecurity governance liability. Courts would benefit from concrete benchmarks evaluating director cybersecurity decision-making processes. Shareholders would gain stronger legal tools challenging inadequate governance decisions effectively. This improved accountability framework offers practical applicability across judicial and corporate contexts. Corporate boards would face meaningful incentives prioritizing genuine cybersecurity risk management. Insurance companies would benefit from clearer liability standards supporting accurate risk assessment. Policymakers should prioritize these reforms given increasing ransomware frequency and severity. This research provides meaningful groundwork supporting stronger shareholder protection legal frameworks. Legal reclassification directly addresses this remedy gap through clarified governance accountability standards (Elsayed et al., 2024).

E. Insurance Market Uncertainty Due to Unclear Liability Standards

This finding reveals significant instability within the growing cyber insurance market. Insurers offer ransomware coverage without consistent legal benchmarks for pricing risk. Unclear corporate liability standards make accurate risk assessment extremely challenging currently. Insurance companies struggle balancing competitive pricing against unpredictable claims exposure levels. This uncertainty affects both insurer profitability and policyholder coverage reliability significantly. Some insurers have restricted ransomware coverage due to unpredictable claims patterns. Others have raised premiums substantially, reflecting genuine uncertainty about future losses. Companies purchasing coverage often lack clarity about their actual legal exposure. Recent industry discussions have called for standardized cyber risk assessment frameworks. Regulators have begun examining whether current insurance practices adequately protect policyholders. However, comprehensive regulatory guidance addressing these concerns remains largely underdeveloped currently (He et al., 2025).

This market instability produces meaningful consequences for companies seeking financial protection. Companies face unpredictable premium increases without understanding underlying risk calculation methods. Some businesses find comprehensive ransomware coverage increasingly difficult or expensive obtaining. This difficulty leaves companies financially vulnerable during actual ransomware attack incidents. Weak liability standards also complicate claims processing after attacks occur. Insurers and policyholders frequently dispute coverage terms and liability determinations extensively. These disputes increase costs and delays during already stressful attack recovery periods. Clearer liability standards would help insurers price policies more accurately consistently. Companies would then receive more predictable and reliable coverage terms. This predictability would improve overall corporate financial resilience against ransomware threats. Stable insurance markets remain essential for supporting broader economic cybersecurity preparedness.

Specific industry examples illustrate how liability uncertainty affects insurance practices. Several major insurers reported significant losses following widespread ransomware attack waves. These losses prompted insurers reconsidering coverage terms and pricing structures substantially. Some insurers excluded certain ransomware scenarios entirely from standard policy coverage. This exclusion left companies unexpectedly vulnerable during specific attack circumstances. Claims disputes arose when companies discovered unexpected coverage gaps after attacks. Courts issued inconsistent rulings regarding insurer obligations across different jurisdictions. This inconsistency further complicated insurers' ability to standardize policy terms nationally. Industry groups have proposed standardized definitions for ransomware related liability terms. These proposals suggest growing recognition that current market fragmentation remains problematic. Legal reclassification would provide foundational standards supporting more consistent insurance practices.

This analysis acknowledges certain limitations regarding cyber insurance market research conclusions. Insurance industry data often remains proprietary, limiting comprehensive external research access. This limits researchers' ability to fully analyze pricing and claims patterns. Additionally, insurance markets vary significantly across different countries and regulatory environments. Some markets maintain more mature cyber insurance products than emerging markets currently. These variations complicate creating universally applicable insurance liability standard

recommendations. Furthermore, ransomware tactics continue evolving rapidly, complicating long-term risk assessment models. Insurance standards developed today may require frequent revision as threats change. These limitations suggest reform efforts must remain adaptable to evolving cyber threats.

Comparing insurance approaches across markets reveals interesting contradictions worth examining. Some insurers assume higher premiums alone sufficiently compensate for uncertain risk exposure. Evidence suggests this approach simply shifts financial burden without addressing underlying uncertainty. Other insurers assume restrictive coverage terms adequately protect against unpredictable claims. This approach often leaves policyholders with inadequate protection when attacks occur. These contradictory approaches demonstrate why pricing alone cannot resolve fundamental legal ambiguity. Some regulators assume market competition will naturally produce fair and stable pricing. Evidence suggests uncertainty actually reduces competition as insurers exit challenging markets. This contradiction challenges assumptions that market forces alone ensure adequate consumer protection. These contradictions collectively support arguments favoring clearer statutory liability classification standards.

These findings carry substantial implications for insurers, regulators, and corporate policyholders. Regulators should consider establishing standardized definitions for ransomware related liability terms. Insurers would benefit from clearer risk classification supporting more accurate premium calculations. Companies would gain more predictable and comprehensive coverage protecting against genuine risks. This improved framework offers practical applicability across insurance, regulatory, and corporate contexts. Policymakers should prioritize these reforms given the growing importance of cyber insurance. Legal reclassification directly addresses this market uncertainty through clarified liability standards. Insurance markets would likely stabilize considerably following consistent legal risk classification. This stability would benefit insurers, companies, and shareholders across affected industries. This research provides meaningful groundwork supporting future cyber insurance regulatory development (Călin et al., 2024).

F. Absence of Fiduciary Duty Recognition for Cybersecurity Preparedness

This finding highlights a fundamental oversight within traditional fiduciary duty doctrine. Courts historically developed fiduciary standards addressing financial mismanagement and conflicts of interest. Digital security threats like ransomware rarely appear within these established legal standards. This absence leaves directors without formal obligations regarding cybersecurity preparedness specifically. Boards can technically satisfy fiduciary duties while ignoring genuine cybersecurity risks entirely. This gap creates a troubling disconnect between legal compliance and actual risk management. Companies suffer real damage while directors remain legally protected under outdated standards. Recent corporate governance discussions have begun questioning whether fiduciary duties need updating. Some legal scholars propose extending duty of care explicitly toward cybersecurity oversight. However, courts have not yet formally recognized this extension in major rulings (Hayes, 2026).

This doctrinal gap produces meaningful consequences for corporate risk management practices. Boards lack formal legal pressure requiring genuine cybersecurity oversight and investment. This absence allows some companies treating cybersecurity as optional rather than essential. Directors focus attention on traditional financial risks while overlooking growing digital threats. This imbalance leaves companies vulnerable despite having seemingly compliant governance structures. Recognizing cybersecurity within fiduciary duty would shift this dangerous imbalance meaningfully. Boards would then face genuine legal pressure prioritizing cybersecurity investment decisions. This pressure could substantially improve corporate preparedness against ransomware and similar threats. Companies would likely allocate more resources toward proactive security measures. This shift would ultimately benefit shareholders, employees, and broader corporate stakeholders collectively.

Several examples demonstrate how this doctrinal gap affects real corporate behavior. Companies suffered major ransomware attacks despite having seemingly adequate governance structures formally. Investigations later revealed boards received warnings about vulnerabilities but took minimal action. Courts reviewing these cases found no fiduciary duty breach under current standards. This outcome frustrated shareholders who expected meaningful accountability following clear negligence. Similar patterns emerged across multiple industries facing significant ransomware attack incidents. Legal commentators increasingly criticize courts for failing recognizing modern cybersecurity risks adequately. Some jurisdictions have begun exploring statutory reforms explicitly addressing this gap. These developments suggest growing pressure for formal fiduciary duty expansion. Legal reclassification would provide the doctrinal foundation supporting this necessary expansion.

This analysis acknowledges important limitations regarding fiduciary duty doctrine research conclusions. Fiduciary duty standards vary significantly across different legal systems and traditions. Some jurisdictions maintain

broader interpretations than others regarding director oversight obligations. This variation complicates creating universally applicable cybersecurity fiduciary duty standards. Additionally, courts move cautiously when expanding established legal doctrines significantly. This caution reflects legitimate concerns about creating excessive litigation or compliance burdens. Furthermore, defining adequate cybersecurity preparedness requires technical expertise courts may lack. Judges must balance legal principles against rapidly evolving technical security considerations. These limitations suggest doctrinal reform must proceed carefully and incrementally.

Comparing legal traditions reveals interesting contradictions regarding fiduciary duty scope. Some jurisdictions maintain expansive fiduciary duties covering broad categories of corporate risk. These jurisdictions could more easily incorporate cybersecurity within existing legal frameworks. Other jurisdictions maintain narrower, more specific fiduciary duty definitions historically. These narrower frameworks resist incorporating new risk categories without explicit statutory authorization. This contradiction demonstrates why doctrinal reform approaches must vary across jurisdictions. Some legal scholars argue existing broad duties already implicitly cover cybersecurity preparedness. Others argue explicit statutory recognition remains necessary given the significant financial stakes. This disagreement highlights genuine uncertainty regarding the best reform pathway forward.

These findings carry substantial implications for courts, legislators, and corporate governance reformers. Legislators should consider explicitly extending fiduciary duty standards toward cybersecurity oversight. Courts would benefit from clearer statutory guidance supporting doctrinal expansion confidently. Corporate boards would gain concrete legal incentives prioritizing genuine cybersecurity preparedness investments. This clarified framework offers practical applicability across judicial, legislative, and corporate contexts. Shareholders would gain stronger legal grounds for holding negligent boards accountable. Insurance companies would benefit from clearer standards supporting more accurate risk assessment. Policymakers should prioritize this reform given increasing ransomware frequency and severity. This research provides meaningful groundwork supporting future fiduciary duty doctrine development (Teichmann, 2026).

G. Implication

This research challenges traditional legal theories treating criminal law and corporate governance separately. Classical fiduciary duty frameworks focus narrowly on financial mismanagement rather than digital security threats. These findings suggest cybersecurity preparedness deserves formal recognition within established governance theory. This shift would strengthen accountability while creating new compliance obligations for corporate boards. Positive outcomes include stronger shareholder protection, clearer director duties, and improved insurance market stability. Negative consequences might include increased litigation risk and higher compliance costs for smaller companies. Regulators could use these findings designing unified disclosure requirements and enforcement mechanisms internationally. Current legal frameworks remain fragmented, inconsistent, and poorly suited addressing modern digital threats effectively. Real-world application requires courts recognizing cybersecurity negligence within existing fiduciary duty standards. Policymakers might introduce mandatory board-level cybersecurity expertise requirements and standardized reporting timelines. Corporate boards, shareholders, insurers, and regulators would all benefit from this clarified framework. Recent initiatives, including proposed European Union cybersecurity directives, reflect growing momentum toward reform. Smaller companies with limited resources may struggle meeting stricter compliance obligations initially. Jurisdictional differences and rapidly evolving ransomware tactics remain significant obstacles requiring ongoing legal adaptation. This research provides theoretical grounding supporting practical legal reform across multiple stakeholder groups.

CONCLUSION

Global corporations face escalating financial and reputational damage from ransomware attacks annually. This research examined how legal systems classify ransomware primarily as criminal conduct. Treating ransomware exclusively as crime overlooks serious corporate governance and accountability failures. Directors currently lack clear duties regarding cybersecurity preparedness and incident disclosure obligations. Shareholders similarly lack effective legal remedies challenging inadequate board cybersecurity oversight decisions. Insurance markets struggle pricing risk without consistent legal liability standards across jurisdictions. These interconnected gaps demonstrate why ransomware deserves formal recognition as corporate risk. Recent regulatory discussions, including proposed cybersecurity disclosure rules, reflect growing awareness of these gaps. However, meaningful legal reform remains slow, fragmented, and inconsistent across different countries. This research connects criminal law, corporate

governance, and financial regulation within one coherent framework. Digital threats continue growing more sophisticated, making this legal gap increasingly urgent addressing.

Three central arguments emerged throughout this research supporting formal legal reclassification. First, courts rarely recognize cybersecurity negligence within traditional fiduciary duty frameworks. Second, disclosure requirements vary significantly across jurisdictions, creating inconsistent shareholder protection. Third, insurance markets remain unstable without clear corporate liability standards guiding risk assessment. These arguments collectively demonstrate systemic weaknesses spanning multiple interconnected legal domains. Addressing one gap alone would prove insufficient without comprehensive coordinated reform efforts. Legal reclassification offers a unifying framework connecting these previously fragmented regulatory areas. This approach strengthens accountability while providing clearer guidance for corporate decision-makers. Stronger frameworks would benefit shareholders, employees, insurers, and broader financial market stability. This research demonstrates why isolated legal reforms cannot adequately address modern cybersecurity threats. A comprehensive approach remains essential for achieving genuine corporate accountability improvements.

These findings carry meaningful implications extending beyond academic legal scholarship alone. Policymakers could use this research designing unified international cybersecurity disclosure standards. Corporate boards could apply these findings strengthening internal cybersecurity governance structures immediately. Regulators might introduce mandatory cybersecurity expertise requirements for corporate board members. Courts could reference this framework when evaluating director conduct during litigation. Future research should examine how specific reclassification proposals perform across different legal systems. Researchers might also study how emerging technologies affect evolving ransomware attack methods. Additional studies could explore practical implementation challenges facing smaller companies specifically. This research provides a foundation supporting continued scholarly and policy development efforts. Addressing these gaps remains essential for building genuinely resilient corporate governance systems worldwide.

BIBLIOGRAPHY

Andre Yosua, M., &Hardianto, S. (2024). The role of criminal law in combating corporate crime that harms the public interest. *Global International Journal of Innovative Research, 2*(11), 2616–2625. https://doi.org/10.59613/global.v2i11.364

Ashraf, M., & Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review, 98*(4). https://doi.org/10.2308/TAR-2020-0787

Bello, A.-W., Wonuola, I., Izundu, A. C., &Izundu, J. C. (2025). Cybersecurity threats in the financial sector: Analyzing attack types, vulnerabilities, and response mechanisms across geopolitical contexts (2015–2024). *International Journal of Science and Research Archive, 16*(1), 134–150. https://doi.org/10.30574/ijsra.2025.16.1.2007

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), 115. https://doi.org/10.1186/s43093-024-00402-9

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

Hayes, C. (2026). Evolving threats, evolving duties: Ransomware, artificial intelligence, and cybersecurity law. *Case Western Reserve Journal of Law, Technology & the Internet, 17*(1), A5. https://scholarlycommons.law.case.edu/jolti/vol17/iss1/5

Hayes, C. (2026). Evolving threats, evolving duties: Ransomware, artificial intelligence, and cybersecurity law. *Case Western Reserve Journal of Law, Technology & the Internet, 17*, A5. https://scholarlycommons.law.case.edu/jolti/vol17/iss1/5

He, Q., Faure, M., & Chen, C. Y. (2025). Insuring the "uninsurable" cyberwarfare: Rethinking war exclusions in cyber policies and the role of insurance in global cybersecurity governance. *The Geneva Papers on Risk and Insurance – Issues and Practice, 50*, 470–501. https://doi.org/10.1057/s41288-025-00346-3

Irvita, M., & Asriani, A. (2025). Transparency and accountability in the justice system: Building public trust and justice: The role of public trust in fair law enforcement. *Priviet Social Sciences Journal, 5*(4), 26–40. https://doi.org/10.55942/pssj.v5i4.367

Jaffe, J., &Floridi, L. (2024). *Ransomware*: Why it's growing and how to curb its growth. *Applied Cybersecurity & Internet Governance*. https://doi.org/10.60097/ACIG/192959

Khan, M. N. I., & Rabbi, M. S. (2024). Cybercrime, legal accountability, and contractual risk: A systematic review of jurisprudence and protective frameworks. *American Journal of Advanced Technology and Engineering Solutions, 4*(1), 71–100. https://doi.org/10.63125/228bwz17

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

Phipps, A., & Nurse, J. R. C. (2025). Inside ransomware groups: An analysis of their origins, structures, and dynamics. *Computers & Security*. Advance online publication. https://doi.org/10.1016/j.cose.2025.104705

Qureshy, A. (2023). Director duties and shareholder protection within the modern enlightened paradigm. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4630607

Rakha, N. A. (2022). Significance of regulation for enhancing online activity. *Web of Scientist: International Scientific Research Journal, 3*(5), 1854–1859.https://api.ziyonet.uz/uploads/books/10001253/cbgt9bl0j0Inb1j.pdf

Rakha, N. A. (2023). Artificial intelligence strategy of Uzbekistan: Policy framework, preferences, and challenges. *International Journal of Law and Policy, 1*(2). https://doi.org/10.59022/ijlp.27

Simanjuntak, S. Y., & Waluyo, B. (2025). Criminal liability for hacking personal data through ransomware attacks on digital service providers in Indonesia. *Jurnal Daulat Hukum, 8*(4), 851. https://doi.org/10.30659/jdh.v8i4.48885

Song, Y., Sheedy, E. A., & Yu, F. (2026, June 10). Voices from Australian industries: Understanding cybersecurity disclosure *(SSRN Working Paper No. 6909958). SSRN*. https://doi.org/10.2139/ssrn.6909958

Tariq, A. (2025). Mandatory sustainability reporting and the disclosure-performance gap: Insights from the EU directive. *Meditari Accountancy Research*. Advance online publication. https://doi.org/10.1108/MEDAR-02-2025-2838

Teichmann, F. (2026). International legal responses to ransomware: Toward a ban on payments? *International Cybersecurity Law Review, 7*, 41–68. https://doi.org/10.1365/s43439-025-00167-z

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

Tsohou, A., Diamantopoulou, V., Gritzalis, S., &Lambrinoudakis, C. (2023). Cyber insurance: State of the art, trends and future directions. *International Journal of Information Security, 22*(3), 737–748. https://doi.org/10.1007/s10207-023-00660-8

Umeanozie, C. P., & Akana, C. (2025). Cybersecurity and critical infrastructure: Legal obligations under the Cyber Incident Reporting for Critical Infrastructur*e Act, 2022*.

Vidović, N., Cvetković, V. M., Beriša, H., &Milašinović, S. (2025). Understanding ransomware through the lens of disaster risk: Implications for cybersecurity and economic stability (Preprint). https://doi.org/10.20944/preprints202504.1950.v1