CIVIL LIABILITY FOR CYBER HARM: INTERNATIONAL AND COMPARATIVE APPROACHES

Yorkinova Sangina Yahyo kizi
Master's student at Tashkent State Law University
E-mail: [yorkinovasangina@gmail.com]
https://doi.org/10.5281/zenodo.15805915

ARTICLE INFO

Qabul qilindi: 25-Iyun 2025 yil
Ma'qullandi: 28-Iyun 2025 yil
Nashr qilindi: 30-Iyun 2025 yil

KEYWORDS

Cyber harm; civil liability; cybersecurity regulation; DORA; NIS2; Online Harms Act; digital fiduciaries; strict liability; Uzbekistan cyber law; hybrid regulation; data protection; platform accountability; international law; digital risk governance; information harm

ABSTRACT

This article explores the evolving landscape of civil liability for cyber harm through international, comparative, and national lenses, focusing on developments from 2022 to 2025. It examines how legal systems are redefining responsibility in the digital age, with an emphasis on regulatory obligations, civil remedies, and conceptual innovations. International frameworks like the EU's DORA, CRA, and NIS2, along with OECD recommendations, establish risk-based accountability for cyber resilience. Comparative analysis highlights diverse national approaches in Canada, the UK, Singapore, and others—ranging from statutory duties for platform safety to cybersecurity certification regimes. Uzbekistan's legal transformation is presented as a dynamic case study of emerging liability models in developing jurisdictions. The article also integrates academic theories on digital harm, strict liability, digital fiduciaries, and hybrid regulatory models, revealing a shift toward proactive and preventive legal standards. This synthesis contributes to understanding how legal doctrine, regulatory design, and technology interact to shape a maturing civil liability regime for cyber risks worldwide.

Introduction

"Cyber harm" encompasses a broad range of injuries arising from digital activities – from data breaches and disruptions of critical systems to online harassment and misinformation. As society becomes more dependent on digital infrastructure, legal systems worldwide are grappling with how to allocate responsibility and liability for these harms. Recent years (2022–2025) have seen intensified efforts at multiple levels – international frameworks, national legislation, and academic discourse – to develop robust approaches to **civil liability for cyber harm**. This includes regulatory initiatives (e.g. the EU's Digital Operational Resilience Act), comparative national laws (e.g. Canada's proposed Online Harms Act, Singapore's cybersecurity certification regime), emerging legal theories (e.g. *digital harm*

and *information harm*, strict liability for digital risks, *digital fiduciary duties*), hybrid public-private regulatory models, and specific developments in countries like Uzbekistan. This synthesis provides an organized overview of these developments, laying a foundation for a comprehensive academic analysis.

International Frameworks and Institutional Initiatives

International and multi-jurisdictional bodies have advanced several frameworks to address cyber resilience and accountability. Notably, the **European Union's Digital Operational Resilience Act (DORA)** was adopted in 2022 (Regulation (EU) 2022/2554) to bolster the financial sector's ability to withstand and respond to ICT-related disruptions. Effective January 17, 2025, DORA imposes uniform requirements on banks, insurers, investment firms and other financial entities to implement robust cyber risk management, incident reporting, digital operational resilience testing, and oversight of third-party ICT service providers. By harmonizing rules across member states, DORA aims to prevent cyber incidents from undermining financial stability; it explicitly holds board-level management accountable for ICT risk and does not preclude further civil or criminal liability for failures.

The EU has also proposed the **Cyber Resilience Act (CRA)**, focusing on cybersecurity of products with digital elements. While still under negotiation, the CRA would require manufacturers to ensure software and IoT products meet cybersecurity standards throughout their lifecycle. Significantly, the CRA's latest text encourages Member States to shield good-faith cybersecurity researchers from legal liability – recommending non-prosecution and exemption from civil liability for ethical hacking activities, which in some jurisdictions might otherwise trigger claims. This reflects a growing recognition that vulnerability disclosure is vital for cyber defense, and legal frameworks should not perversely punish researchers who help identify flaws.

Beyond the EU, international organizations like the **OECD** have been active in shaping principles for cyber accountability. In late 2022, the OECD Council adopted several Recommendations on digital security policy. Of particular relevance is the **OECD Recommendation on the Digital Security of Products and Services (2022)**, which responds to "market failure" in the cybersecurity of software and hardware products. The OECD noted that suppliers often lack incentives to invest in security, leading to systemic risk. The Recommendation urges governments to realign incentives by placing a *"duty of care"* on technology suppliers for the security-by-design of their products. In other words, manufacturers and service providers should bear responsibility – potentially including liability – for vulnerabilities in their products, and ensure timely patches and secure lifecycle practices. The OECD also calls on governments to encourage coordinated vulnerability disclosure and provide **safe harbors for ethical hackers**, protecting them from undue legal threats. These international best practices lay the groundwork for stricter liability standards: if a company fails to exercise due care in securing its digital products, it could be held liable for resulting harms, much as in traditional product liability law. Indeed, the **G20** has echoed some of these themes. G20 leaders have repeatedly emphasized the importance of cyber resilience and common standards. For example, the 2023 G20 Leaders' Declaration welcomed the Financial Stability Board's recommendations to achieve greater convergence in cyber incident reporting across jurisdictions. By harmonizing incident reporting and terminology (e.g. via the FSB's Cyber Lexicon and "FIRE" incident reporting exchange format), G20

members seek to improve transparency and facilitate cross-border accountability for cyber incidents. While such high-level declarations do not impose liability directly, they signal political support for frameworks where both public authorities and private entities share responsibility for managing cyber risks.

Another domain of international discussion is **hybrid regulation** models that combine public regulation with private-sector co-regulation. Bodies like the OECD have highlighted the need to balance economic/social incentives with traditional national security approaches in cybersecurity policy. The concept of "hybrid" or co-regulation appears in the context of online content as well (discussed below): regulators increasingly require platforms and companies to police themselves under oversight – effectively deputizing private actors to fulfill public policy goals. This blend of **public and private responsibility** is evident in many new laws addressing digital harms and is discussed further in theoretical models below.

Comparative National Approaches to Cyber Liability

Different countries have adopted diverse legal strategies to address cyber harm and allocate liability. A comparative survey reveals evolving legislative measures in areas like platform regulation, critical infrastructure protection, and consumer protection in the digital realm:

Canada. In Canada, recent efforts have bifurcated into two streams – one targeting **online content harms** and another focusing on **cybersecurity of critical systems**. On the content side, the federal government introduced Bill C-63 (the **Online Harms Act**) in February 2024. This legislation (also referred to by commentators as a "Digital Harm Accountability Act") would impose obligations on online platforms (including social media, live-streaming services, and adult content sites) to act responsibly and **mitigate users' exposure to harmful online content**. It establishes a **Digital Safety Commission** and an Ombudsperson to enforce duties such as a duty to act responsibly, a duty to protect children with age-appropriate design, and a duty to remove or block certain extreme content (e.g. child sexual exploitation and violent hate content). While primarily a regulatory regime (enforced by fines and binding orders), this framework enhances platforms' accountability and could indirectly influence civil liability by setting a standard of care for content moderation. Notably, the Bill's backgrounder emphasizes that platforms have for too long "offloaded their responsibilities" onto users and parents, and that the law will **hold platforms accountable** for the harms they "create or amplify". In parallel, Canada has advanced legislation to bolster cybersecurity in critical infrastructure: Bill C-26, the proposed **Critical Cyber Systems Protection Act (CCSPA)**. Introduced in June 2022, this Act would impose mandatory cyber risk management measures on federally regulated sectors (like finance, telecom, energy, and transport) and grant regulators inspection and enforcement powers. Non-compliant companies could face heavy administrative penalties. Although CCSPA is about regulatory compliance rather than private lawsuits, it reflects a trend of using public law to force private entities to prevent cyber harm. Additionally, Canada's privacy law reforms (Bill C-27, Digital Charter Implementation Act) propose a new private right of action for data breaches, potentially expanding civil liability for companies that fail to protect personal information. Thus, Canada is pursuing both ex ante regulation (to prevent harm) and ex post liability (to compensate harm) in the digital sphere.

United Kingdom. The UK has recently enacted the **Online Safety Act 2023**, a sweeping law that creates a statutory **duty of care** for providers of online platforms and search engines. Companies must take action to prevent both illegal content and certain legal-but-harmful content (particularly content harmful to children) from proliferating on their services. The Act empowers Ofcom (the UK communications regulator) to enforce these duties, including issuing codes of practice and imposing fines up to the greater of £18 million or 10% of global turnover for non-compliance. While the duty of care is enforced administratively, the law fundamentally shifts the liability landscape: it essentially holds platforms liable (via regulatory sanctions) if they **fail to take reasonable steps to mitigate online harms**. Notably, the Act also contemplates "technological solutions" like scanning encrypted messages for child abuse content – a controversial requirement raising privacy concerns. The UK approach exemplifies hybrid regulation: it mandates corporate responsibility and robust internal systems for user safety, with government oversight, rather than relying on individual victims to bring civil lawsuits. However, by establishing clear duties, it could influence civil negligence claims (e.g. if a platform egregiously fails its duty and harm results, users might cite the statutory duty in litigation). The UK is also looking beyond content to cybersecurity of consumer products: the **Product Security and Telecommunications Infrastructure Act 2022** introduces minimum security requirements for IoT devices (e.g. banning default passwords and requiring vulnerability disclosure policies), backed by fines for manufacturers. This aligns with the EU and OECD philosophy that product makers should bear responsibility for cyber vulnerabilities.

Singapore. Singapore is recognized for its advanced cybersecurity regime, which emphasizes both regulatory compliance and capacity-building. The **Cybersecurity Act 2018** (amended 2024) establishes a legal framework for protecting critical information infrastructure (CII) and empowers the Cyber Security Agency (CSA) to issue standards and directives. Recent amendments in 2024 expanded the Act's scope to cover new threats and sectors. Notably, Singapore has pioneered a **certification scheme for cybersecurity readiness** in the private sector. The CSA administers the **Cyber Essentials** and **Cyber Trust** certification marks – frameworks that define baseline and advanced cybersecurity practices for organizations. In April 2025, the Monetary Authority of Singapore (MAS) and CSA announced they are considering **making these certifications mandatory for vendors** who seek to be licensed or bid on government contracts involving sensitive data. This move was prompted by a major data breach at a third-party vendor, underscoring supply-chain cyber risks. Requiring vendors to attain Cyber Essentials/Trust certification would effectively impose a **duty of due care**: a vendor's failure to implement "adequate cybersecurity measures" (as evidenced by lack of certification) could be grounds for contractual liability or exclusion from business opportunities. In Singapore's financial sector, regulators already expect stringent oversight of outsourced service providers. The broader trend is a **prophylactic approach** – instead of waiting for cyber harm to occur and then assigning liability, Singapore sets high ex ante standards and **accredits organizations** that meet them. While direct civil litigation for cyber incidents in Singapore is still nascent, these regulatory standards could inform negligence claims (e.g. if a certified organization suffers a breach, loss of certification or violation of standards could be evidence of negligence).

European Union. Aside from DORA and the CRA, the EU in 2022 also adopted the **NIS2 Directive (Directive (EU) 2022/2555)**, which updates its cybersecurity law for critical infrastructure and essential services. NIS2 mandates that a wide range of companies (from energy and transport to health, digital providers, and even certain manufacturing sectors) implement cybersecurity risk management and incident reporting, under threat of administrative fines. While primarily a public-law enforcement scheme, NIS2 explicitly permits **affected parties to seek damages**. By requiring "appropriate" cybersecurity measures, it sets a benchmark that could be used in civil negligence lawsuits if a company's inadequate security leads to damage. Furthermore, the EU is revising its **Product Liability Directive** to encompass digital products and software. A proposal in 2022 would ensure that victims can claim compensation for damage caused by defective software, including vulnerabilities (for example, if insecure software in a connected device causes property damage or personal injury) – effectively extending strict products liability to digital products. Alongside, an **AI Liability Directive** has been proposed to ease the burden of proof on individuals harmed by AI systems, introducing a rebuttable presumption of causality when providers violate certain AI safety obligations. These European moves illustrate a tightening nexus between **regulatory non-compliance and civil liability**: failure to follow cybersecurity or AI regulations could not only incur fines but also make it easier for victims to prevail in civil suits.

Other Jurisdictions. Several other countries are developing notable cyber liability regimes. **Australia**, for instance, has seen heightened scrutiny of directors' duties regarding cybersecurity after a landmark 2022 Federal Court case (ASIC v RI Advice Group). In that case, a financial services firm was found to have breached its license obligations by failing to manage cybersecurity risks; the court underscored that cybersecurity is now a board-level responsibility. Following this, Australian regulators have warned that corporate officers could violate their fiduciary duties (duty of care and diligence) if they neglect cyber-risk governance. This has led to discussions of *de facto* **digital fiduciary duties** for directors – i.e. treating cybersecurity oversight as part of the duty to act in the company's best interest. Similarly, **New York State** (USA) has imposed rigorous cybersecurity regulations on financial institutions (the NY DFS Cybersecurity Regulation) which include potential liability for certifying falsely on compliance. **Israel** has a sophisticated cyber ecosystem, and while its laws rely on existing tort and contract principles for cyber incidents, the government plays an active role through its National Cyber Directorate in setting mandatory standards for critical sectors (blurring the line between guidance and legal obligation).

Content vs. Infrastructure Approaches. It is worth noting the divergence in how legal systems approach **online content harm** versus **technical cybersecurity failures**. Countries like Canada, the UK, Australia, and the EU are all enacting laws for platform content accountability (hate speech, misinformation, child protection), which operate via regulatory duties and fines rather than traditional tort liability. On the other hand, when it comes to data breaches, ransomware, or infrastructure outages caused by cyberattacks, the trend is toward either (a) regulatory enforcement (penalizing companies for not preventing the incident) or (b) facilitating private class actions (especially in jurisdictions like the United States). In the U.S., while there is no comprehensive federal cyber liability law, there's been a surge of data breach lawsuits and consumer protection actions by the FTC. Some scholars have even

advocated for **strict liability for data breaches** to better incentivize companies – arguing that firms should internalize the full costs of cyber incidents. For example, Cooper and Kobayashi (2022) propose a strict liability regime for companies' data security failures, reasoning that this would force firms to take socially optimal precautions and could be coupled with cyber insurance to spread the risk. Although the U.S. has not adopted that approach broadly, certain sectors have quasi-strict obligations (e.g. under healthcare and financial data regulations), and the idea underscores a possible future direction in comparative law.

Academic Discourse on Digital Harm and Liability

Recent scholarly work provides conceptual underpinnings for these legal developments. Researchers and theorists are actively debating how traditional legal principles – like harm, duty, and liability – should evolve in the **digital environment**:

Conceptualizing "Digital Harm" and "Information Harm". One notable thread is defining the nature of harms in the digital age. The lexicon of "digital harm," "data harm," "cyber harm," and "algorithmic harm" has expanded to capture injuries that are often intangible. Unlike physical harm, digital harms can include the wrongful collection or exposure of personal data, the spread of disinformation that erodes societal trust, or interference with information systems. These often do not fit neatly into traditional tort categories. *Legal scholars argue that the law's understanding of harm needs to broaden* to encompass not just direct financial loss, but also **dignitary harms, privacy harms, and collective harms** (e.g. harms to societal interests in fair information flows). For instance, a massive personal data breach might not cause immediate monetary loss to each individual, but it inflicts a loss of privacy and security – an "information harm" that current legal remedies struggle to address. Academic commentary (e.g. Citron, Waldman, Solove) has pressed for recognizing privacy violations and data misuse as cognizable injuries, sometimes arguing for statutory damages or new causes of action to sidestep the problem of proving harm. This academic pressure is partially reflected in laws like the California Consumer Privacy Act (which provides statutory penalties for data breaches even absent specific damage) and in European GDPR's allowance for compensation for non-material damage. In sum, scholars are shaping a narrative that **cyber harms are real harms** – even if they challenge conventional damage models – thereby justifying innovative liability approaches to redress them.

Strict Liability in Digital Context. In product liability law, strict liability holds manufacturers liable for defects regardless of fault. Some scholars propose an analogous approach for digital products and services. The rationale is that software flaws or security vulnerabilities are akin to product defects. If insecure software causes foreseeable harm (like enabling a hack or causing a device failure), the maker should be liable to victims without the victim needing to prove negligence. Proponents argue this would shift the cost of cyber risks onto those best placed to reduce them (the developers and vendors) and correct the current under-investment in security. As noted, an academic article by Cooper & Kobayashi (2022) finds that firms do not internalize the full cost of data breaches under the current negligence-based system, and suggests strict liability would incentivize optimal security and also stimulate a market for cyber insurance to price the risk. We see echoes of this theory in the OECD's duty-of-care recommendation and the EU's expansion of product liability to software.

Another area of discussion is whether **AI-related harms** should be subject to strict liability, given the difficulty for users to prove how an algorithm caused damage. The proposed EU AI Liability Directive leans in this direction by easing the burden of proof on the injured party (a step short of full strict liability). Overall, while strict liability for digital harms is not yet the norm, academic dialogue is pushing lawmakers to consider it for high-risk contexts, on the premise that it may be more efficient and equitable in an era of complex, opaque technologies.

"Digital Fiduciary Duty" and Information Fiduciaries. Another rich concept in recent scholarship is applying fiduciary principles to digital relationships. Traditionally, fiduciary duty arises in contexts like doctor-patient or lawyer-client, where one party has significant power over the other's interests, demanding duties of loyalty and care. Some scholars (e.g. Jack Balkin) have argued that large online service providers (social media companies, search engines, cloud providers) act as **"information fiduciaries"** for their users. Users entrust platforms with personal data and attention, creating a power imbalance. Thus, the argument goes, these companies should have a *fiduciary-like legal duty* to not misuse user data and to act in users' best interests, at least with respect to core functions (e.g. handling of personal information). This concept has gained traction: for example, the EU's **Data Governance Act 2022** creates a class of **"data sharing intermediaries"** who must act as neutral custodians of data with fiduciary duties (they cannot exploit the data for other purposes). In the U.S., a **Data Care Act** was proposed in 2021–2022 to impose duties of loyalty, confidentiality, and care on online companies regarding user data. While that bill has not passed, several U.S. states (e.g. Illinois in debates on biometric data, and broad discussions in privacy law reforms) have flirted with the idea of imposing heightened duties on data collectors. Relatedly, corporate law scholars like Robert Walters (2023) discuss **directors' fiduciary duties** in relation to cybersecurity and data governance. The Australian case mentioned earlier (RI Advice 2022) implies that failing to address cyber risks could be a breach of directors' duty of care to the company. Globally, this suggests an emerging doctrine of **digital fiduciary duty** at multiple levels: corporate leaders must treat cybersecurity as part of their fiduciary oversight, and digital service providers might owe quasi-fiduciary obligations to users. If recognized in law, this could significantly expand civil liability – for instance, a user could potentially sue a platform for breaching a duty of loyalty by using their data in exploitative ways (whereas today such claims face hurdles under contract and tort law). Though still largely theoretical, the fiduciary model is a compelling solution to the problem of trust and power asymmetry in the digital economy.

Hybrid and Multi-Stakeholder Regulatory Models. Scholars are also examining *"hybrid regulation"* as a theoretical model for governing digital risks. Traditional command-and-control regulation by government may be too slow or clumsy for the fast-moving tech sector, whereas pure self-regulation by industry often fails to protect public interests. Hybrid models seek a middle ground – for example, **co-regulation**, where industry develops standards or codes of practice that are then enforced or endorsed by a government regulator. The EU's approach in areas like the **Digital Services Act (2022)** exemplifies this: platforms must assess systemic risks on their services and implement measures, and regulators supervise these efforts. In cybersecurity, some propose **public-private partnerships** where governments share threat intelligence with industry and in return companies meet certain security baselines. A 2022 OECD paper stressed coordinating economic policy tools (like

insurance markets, disclosure requirements) with traditional cybersecurity efforts. Another aspect is **liability sharing** between public and private actors – for instance, if a cyber incident is due to state-sponsored hacking, should the state bear some responsibility, or should private companies be solely liable to customers? This edges into the debate on cyber insurance backstops and government indemnification for extreme events (similar to terrorism insurance pools). In sum, theoretical models suggest that optimal regulation of cyber harm likely involves **multiple layers**: industry self-governance, market mechanisms (insurance, audits), and overarching legal duties set by the state. Liability in such models might be distributed: e.g., a baseline of strict liability on companies for preventable harms, coupled with safe harbors if they adhere to certified standards (a form of regulated immunity), and residual state compensation for certain large-scale harms. While still developing, these hybrid notions are evident in practice – for example, *New Zealand's approach to online content harm* uses a government e-safety commissioner alongside industry codes; *France's SECNUM certification* encourages companies to get cyber-certified; and *the U.S. DHS's SAFETY Act* provides liability protections for certified anti-terrorism technologies, an idea that some have suggested extending to cybersecurity products.

Uzbekistan's National Developments in Cybersecurity Liability

Uzbekistan provides a case study of a country rapidly updating its legal framework to address cyber threats, with a notable emphasis on liability and enforcement in recent presidential decrees. The **Law of the Republic of Uzbekistan "On Cybersecurity" (No. ORQ-764)** was adopted in April 2022 and took effect July 17, 2022. This foundational law defines the principles of cybersecurity and establishes obligations for operators of "critical information infrastructure" across various sectors (from finance and health to energy and ICT). Under the Law, critical facility operators must comply with technical cybersecurity requirements set by the state security service, implement continuous monitoring and incident response systems, undergo certification, and allow government inspections. These obligations are preventative; the law itself does not spell out civil liability to private parties, but non-compliance can lead to administrative sanctions.

Building on the 2022 Law, **Presidential Resolution No. PP-167 (31 May 2023)** introduced additional cybersecurity requirements for companies, particularly critical infrastructure. This 2023 regulation mandated detailed compliance steps – such as prompt incident reporting to regulators, assisting in cyber investigations, and ensuring cybersecurity personnel are certified by authorities. Companies must implement robust access controls, auditing mechanisms, malware protection, and data backup for systems handling critical or confidential information. Notably, the resolution requires **certification of critical facilities for cybersecurity compliance**. This effectively ties legal compliance to an audit/certification process. While these measures again focus on prevention, the backdrop is a legal environment where failing to meet these standards could constitute a violation potentially leading to fines or other liability.

The most significant shift comes with the **April 30, 2025 Presidential Decree (No. PQ-153)**, which explicitly aims to **bolster cybersecurity and target cybercrimes**. This decree, as reported by legal analysts, lays the groundwork for stronger liability and enforcement in multiple ways. First, it empowers regulators (notably the Ministry of Internal Affairs) to "name and shame" organizations that have poor cyber safeguards – publishing lists of banks

or companies with the most cybersecurity incidents due to vulnerabilities. This public disclosure can severely damage a company's reputation and potentially expose it to customer lawsuits or loss of business. Second, and crucially, the decree proposes to **introduce liability for noncompliance with cybersecurity requirements *regardless of whether an incident occurred***. In other words, even if no breach or damage has yet happened, a company could be held liable simply for not meeting the mandated security standards. This is a form of **strict regulatory liability** that does not depend on actual harm – its purpose is clearly to incentivize proactive compliance. Third, the decree addresses the scenario of actual cyber harm: if a cybercrime (e.g. a breach or fraud) occurs *due to an organization's inadequate security*, the responsible organization (especially banks, payment service providers, etc.) will be **required to compensate individuals for the material damage** caused. This is a striking provision, effectively establishing a direct civil liability (or a statutory restitution obligation) to victims of cyber incidents. For example, if a bank's poor cybersecurity allows hackers to steal customer funds or data, the bank would have a legal duty to reimburse the victims for their losses. This approach aligns with the principle of making the negligent party bear the cost of harm and protecting consumers from having to shoulder losses they could not prevent. It also mirrors the scholarly call for internalizing cyber costs: Uzbekistan is essentially saying that if you don't secure your systems, you will pay the price of the breach. Additionally, the decree intends to criminalize certain enabling acts (like individuals knowingly allowing their bank accounts or SIM cards to be used in cybercrime), and to incorporate cybersecurity compliance checks into the investigation of cybercrime cases.

Uzbekistan's evolving framework demonstrates how a country can move from basic capacity-building laws to an aggressive stance on liability within a short period. The combination of **mandatory standards, strict liability for noncompliance, mandatory compensation, and reputational sanctions** provides a multifaceted enforcement toolkit. By publicly listing institutions with cyber incidents and imposing compensation duties, Uzbekistan's government is effectively leveraging both **public enforcement and private litigation surrogates** to combat cyber harm. It is noteworthy that these developments are being driven by presidential decrees and resolutions, reflecting the top-down approach often seen in civil law jurisdictions for technology policy. For the purposes of comparative analysis, Uzbekistan's approach can be seen as an attempt to leapfrog into a best-practice regime by borrowing elements from various sources: the strict obligations and fines resemble EU and Singaporean models, the compensation element echoes consumer protection rationales (and perhaps the banking sector's fraud reimbursement norms), and the naming-and-shaming tactic leverages market forces and public pressure. This comprehensive approach may serve as a case study for other countries with developing digital infrastructure on how to rapidly strengthen cyber resilience through law.

Conclusion

Across international and national landscapes, the period 2022–2025 has been marked by **convergence toward stronger accountability for cyber harm**. International bodies like the EU and OECD are setting *de facto* global standards that emphasize risk management duties, resilience, and the shifting of responsibility onto those best able to prevent harm (financial entities, product manufacturers, platform providers). Comparative national efforts reveal an emerging consensus that purely voluntary or after-the-fact remedies are insufficient

– hence the rise of regulatory duties (e.g. duties of care for online safety, mandatory cybersecurity baselines for critical infrastructure) that are enforceable through fines or other sanctions. While these are regulatory in nature, they significantly influence the civil liability environment by defining what is "reasonable" or "responsible" behavior in the digital realm. At the same time, academic thought is enriching these policy moves with new concepts of harm and duty that could, in time, be codified into law: from treating personal data as a subject of fiduciary duty, to imposing strict liability for security breaches, to recognizing novel forms of digital injury. The interplay of **doctrinal innovation** (e.g. information fiduciaries), **technological change** (AI, IoT, etc.), and **practical experience with cyber incidents** (ranging from massive data breaches to online abuse scandals) is driving the evolution of legal norms.

One notable trend is the blending of **public and private remedies** – regulatory frameworks ensure baseline protection and deterrence (often pre-empting harm), whereas civil liability (through courts or statutory compensation schemes) provides avenues for victims to be made whole after harm occurs. For instance, the EU's approach with GDPR fines plus individual damage claims, or Uzbekistan's administrative orders plus mandatory compensation, reflect this two-pronged strategy. Another trend is **preventive accountability**: laws increasingly aim to *prevent* cyber harm through standards and obligations, not just punish it post hoc. This is a departure from traditional tort which is largely reactive. However, as standards tighten, they also pave the way for negligence per se claims and other civil actions when those standards are violated and harm ensues.

In writing a 15-page academic article on this topic, one could organize it in segments similar to above: starting with the international normative framework (to set the stage), then delving into key jurisdictions' approaches (illustrating different models), weaving in academic doctrines to analyze strengths and weaknesses, and perhaps concluding with proposals for an integrated model of cyber liability that marries the best elements of each. The references below provide a selection of recent and authoritative sources – including statutes, regulatory texts, international guidelines, and scholarly writings – that can substantiate and deepen each aspect of the analysis. Together, these sources chronicle a pivotal shift toward a more mature legal handling of cyber risks: one that aspires to not only **assign liability for cyber harm** but ultimately to **reduce and manage digital risks** in the first place, through a fusion of responsibility across public and private spheres.

References:

1. European Union. (2022). Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA). OJ L 333, p.1–79.
2. European Union. (2022). Directive (EU) 2022/2555 (NIS2) of 14 December 2022 on measures for a high common level of cybersecurity across the Union. OJ L 333, p.80–152.
3. European Commission. (2022). Proposal for a Cyber Resilience Act, COM(2022) 454 final. Brussels, Sept. 15, 2022.
4. OECD Council. (2022). Recommendation on Digital Security of Products and Services. OECD/LEGAL/0477, adopted 26 Sept 2022.
5. OECD. (2022). Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities. OECD Digital Economy Papers No. 324.
6. G20 Leaders. (2023). G20 New Delhi Leaders' Declaration (Sept. 10, 2023), Article 46.

7. Financial Stability Board (FSB). (2023). Final Report: Achieving Greater Convergence in Cyber Incident Reporting. Basel, Oct. 2023.
8. Government of Canada. (2024). Bill C-63, Online Harms Act (1st Reading, 44th Parl.). Ottawa: Parliament of Canada.
9. Canadian Heritage. (2024). Backgrounder: Legislation to combat harmful content online (Feb. 26, 2024). Government of Canada News Release.
10. Government of Canada. (2022). Bill C-26, Critical Cyber Systems Protection Act (1st Reading, 44th Parl.). Ottawa.
11. Online Safety Act 2023 (UK), c.50.
12. Department for Digital, Culture, Media & Sport (UK). (2022). Online Safety Bill – Explanatory Notes. London.
13. Cybersecurity Act 2018 (Singapore) (Act 9 of 2018), amended by Cybersecurity (Amendment) Act 2024.
14. Monetary Authority of Singapore & Cyber Security Agency. (2025). Joint Response to The Straits Times Forum Letter on Third-Party Cybersecurity
15. Dentons Law Firm (Ulugbek Abdullaev). (2025, May 14). "Uzbekistan tightens cybersecurity obligations: What businesses need to know." Dentons Insights.
16. Dentons Law Firm (Ulugbek Abdullaev). (2023, June 7). "Uzbekistan: Cybersecurity obligations for companies." Dentons Insights.
17. Dentons Law Firm (Eldor Mannopov & Ulugbek Abdullaev). (2022, April 22). "Uzbekistan adopts cybersecurity law." Dentons Insights.
18. Cooper, J. C., & Kobayashi, B. H. (2022). "Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem." 28 Michigan Technology Law Review 257.
19. Famularo, J. (2023). "Platform-Related Harms." Yale ISP Essays (Information Society Project).
20. Benthall, S. (2022). "For Safe AI Tomorrow, Fiduciary Duties for Big Tech Today." Cornell Tech – Digital Life Initiative Blog.
21. Walters, R. (2023). "Cybersecurity, Data Governance and Directors' Fiduciary Duty: An Expanding Obligation." Australian Business Law Review, 2023(Dec).
22. Balkin, J. et al. (2019). "Information Fiduciaries and the First Amendment." 49 UC Davis Law Review 1183.
23. Lior, A. (2023). "Innovating Liability: The Rise of Insurance in Cybersecurity Governance." 25 Yale Journal of Law & Technology 448. (
24. Jordan, D. & Doshi, R. (2022). "The EU Digital Operational Resilience Act: A New Paradigm for Cybersecurity in Finance." Journal of Cyber Policy 7(3), 429-445.
25. Cyber Peace Institute / UNIDIR. (2022). "Taxonomy of Cyber Harm.