

Research Article

Redefining Fiduciary Oversight in the Digital Age: Board-Level Liability for Intangible Asset Vulnerabilities and Intellectual Property Loss

Oduyebo Tomilayo Olubisi^{1,*} , Akinsola Oluwaseun Kayode¹ , Agboke Mutiu² , Adetoye Funmilola Abeke¹ 

¹Department of Private and Property Law & College of Law, Chrisland University, Abeokuta, Nigeria

²Department of Public Law & Faculty of Law, Fountain University, Osogbo, Nigeria

Abstract

The concept of fiduciary duty has long been framed around safeguarding a company's assets and finances. Corporate governance historically focused on safeguarding tangible property and financial assets. Today, the overwhelming majority of the market capitalisation of the world's largest public companies rests on their balance sheet, and the risks to enterprise value are now far more numerous, from catastrophic loss of intangible assets caused by trade secret cyber-thefts, uncontrolled deployment of generative artificial intelligence (AI) and unmonitored open-source code integration than the risks that the *Caremark Doctrine* was designed to protect against. Originating in Delaware jurisprudence and mirrored in mechanisms under the UK Companies Act 2006, the doctrine of board-level oversight liability has evolved to hold directors strictly accountable for systematic risk management. Today, passively delegating intangible asset risks to IT or legal departments without board-level escalation protocols fails to satisfy good-faith oversight standards. Expanding on recent legal decisions that extend oversight duties to corporate officers, this paper examines global governance failures in the digital age. It proposes a proactive framework that incorporates amended board charters, explicit reporting channels, and specialised insurance reviews to protect intangible assets across international jurisdictions.

Keywords

Fiduciary Duty, Board Oversight, Intangible Assets, Trade Secret, Enterprise Risk Management, Corporate Governance

1. Introduction

1.1. The Intangible Economy and the Anatomy of IP Loss

Over the last fifty years, the makeup of corporate value has turned upside down, a change that does not yet fit within the

fiduciary duty doctrine. In 1975, the proportion of tangible assets, property, plant and equipment, and inventory made up approximately 83% of the market value of the companies in the S & P 500 index, while the intangible assets accounted for

*Correspondence: todayebo@chrislanduniversity.edu.ng (Oduyebo Tomilayo Olubisi)

Received: 16 September 2026; **Accepted:** 29 September 2026; **Published:** 20 October 2026



Copyright: © The Author(s), 2026. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

17% of the market value. [45] This trend had completely reversed by the end of 2025, with intangible assets accounting for about 92% of the market capitalisation, compared to the 17% in 1975, while tangible assets had shrunk to a mere 8%. The book, which has been expanded to include foreign markets, now covers the last 50 years, which the authors call an "economic inversion," and tracks the shift of economic value from tangible to intangible assets [34].

It does not yet appear that this change will be short-lived. This trajectory remained resilient even through global disruption. An interim report from the same study demonstrated that the COVID-19 pandemic failed to reactivate a preference for tangible assets; rather, intangible assets captured more than 90% of the S&P 500's market value by mid-2020, accompanied by a similar, albeit more modest, surge in the S&P Europe 350. [44] While the pandemic's operational disruption was about material supply chains and physical safety in the workplace, boards were governing an increasingly virtual asset base during and after that period. The stability after the global shift and economic shock is itself a sign that the intangible-asset governance gap described in this paper is indeed structural, and that it is unlikely to disappear as the market returns to normal [25].

This shift has not, however, overturned the foundational tenets of corporate board oversight. Modern jurisprudence surrounding board liability for financial fraud and regulatory non-compliance grew out of cases where the vulnerable assets were tangible or statutory namely cash, inventory, or regulatory licenses. [6] The loss of intellectual property is a different form of harm. [6] A trade secret, once leaked, cannot be restored in the same manner as a cash balance; a training corpus that infringes copyrights, once used to train a deployed machine-learning model, cannot be deleted without retraining the model from scratch; an open source violation, once given to millions of end users, cannot be corrected internally. [45] The loss resulting from an IP failure is inherently irreversible - a reality that exposes a fundamental weakness in traditional fiduciary duty doctrine. Because existing governance frameworks rely on the assumption that boards can detect and remedy breaches before permanent harm occurs, they are ill-suited to address damages that are, by nature, unfixable.

1.2. The Governance Gap: Traditional Board Oversight Vs Modern IP Vulnerabilities

Conventional board oversight arrangements, stock exchange-listing requirements for an audit committee and compliance reporting by general counsel came into being to monitor the integrity of financial statements and regulatory compliance. [43] Today's IP issues do not quite fit into any of these categories. In most cases, the first clue of an IP breach or a trade secret cyber-theft will be from an information security team reporting to a chief information security officer (CISO), who might report to several levels below the board, and who,

as the SolarWinds [17] case demonstrated, may not always report a threat in a fashion that is commensurate with the threat itself. [36] Choices with respect to Generative AI deployment are often made by a product/engineering team, based on speed-to-market considerations or technical feasibility, and, if consulted, only after a model has been trained on contested sets of data. [2, 42] Open-source code integration occurs regularly at the granular level of software commitment and is hard to observe from a board level, even when there are legally relevant licence considerations. [10] Each of these vulnerabilities stems from a shared governance failure: while the risk is real and material, and actively monitored by operational teams below the board level, it lacks a dedicated oversight architecture comparable to those long established for financial and safety risks.

The Delaware Supreme Court addressed this governance deficit in *Marchand v Barnhill* [13] holding that board oversight requires an active "board-level compliance reporting system" tailored to a firm's central mission-critical risks. Although *Marchand* arose in the context of food safety - where an ice cream manufacturer suffered a catastrophic listeria outbreak - the court made clear that mere formal compliance with industry regulations does not fulfil a board's fiduciary duties when core operational hazards are at stake. The analogy to intangible-asset governance is clear: if a firm, the market value of whose business is basically intangible, has no cyber-espionage reporting system, no system of tracking the provenance of the data used for AI training and no system for compliance with open-source licences on its board, then it is doubtless currently exposed to the same kind of oversight risk that the Blue Bell board was when it was aware of the listeria contamination.

1.3. Thesis Statement and Structural Roadmap

This paper posits that in an enterprise whose value is overwhelmingly intangible, the fiduciary duty of oversight demands that directors actively exercise their best judgment in establishing, monitoring, and periodically reviewing enterprise-wide IP risk management systems. Consequently, passive reliance on lower-level IT or legal personnel can no longer serve as a "get-out-of-jail-free" card for directors and officers when a catastrophic IP loss occurs - marking what this article terms a new *Caremark* era. [6, 8, 38] Part 2 of the paper follows the doctrinal development of the oversight duty from *Graham v Allis-Chalmers* [3] to *Caremark*, to *Stone v Ritter* [18], to *Marchand*, and the recent extension of the oversight duty to corporate officers in *In re McDonald's Corp.*, to the duties under the Companies Act 2006 codified in the UK.

In Part 3, the paper takes a closer look at three specific examples of contemporary IP vulnerabilities: trade secret cyber theft, the deployment of generative AI, and open-source, unmonitored use. [8] The paper explains in Part 3 how these specific examples can be seen as instances of governance failure. In Part 4, IP risk management is discussed in the context of the business judgment rule, and the chapter also explores the

concept of director and officer insurance. [1] In Part 5, the paper suggests a viable set of revisions to the board charter and escalation mechanisms, before concluding with an argument that the proper interpretation of IP oversight should be that it is a non-delegable fiduciary duty.

2. Evolution of Board Oversight Duties

2.1. The Foundation of Directors' Liability: Duty of Care and Loyalty

Historically, company law recognised corporate directors' duties as primarily comprising two main pillars: the duty of care (requiring directors to exercise diligence and attention in decision-making) and the duty of loyalty (requiring directors to act strictly in the corporation's best interests rather than their own). The board's duty of oversight, however, developed along a far more complex doctrinal path. Initially, the legal standard for board oversight was largely passive and permissive. Under early common law jurisprudence, directors were under no general obligation to proactively install internal monitoring systems to catch corporate wrongdoing in the absence of obvious warning signs or "red flags." This reactive approach meant that unless suspicious activity was brought directly to their attention, directors could not be held liable for failing to uncover employee misconduct.

The oversight duty has an odd doctrinal pedigree, as it stemmed from an application of the duty of care in *Graham v Allis-Chalmers Manufacturing Co*, where the Court said that, apart from an interest in discovering a state of affairs the directors had no reason to suspect was wrongful, they had no duty to create and run a system of corporate espionage. [3] Unfortunately, that permissive standard was not easily put into practice in the more complex, multi-divisional structures of today's corporations, because the Board of Directors of a company cannot manage every decision of its operational divisions, a problem which Chancellor Allen faced head-on in 1996 in *In re Caremark International Inc Derivative* [33].

As corporate structures grew increasingly vast and decentralised, this passive framework proved inadequate for modern corporate governance. A board of directors supervising a multi-divisional enterprise cannot directly manage daily operational choices, making proactive risk monitoring essential. Consequently, modern legal standards evolved from a passive "red flag" requirement into an active, affirmative duty. Today, director oversight requires boards to ensure that information and reporting systems are implemented and monitored to ensure material risk and legal compliance are routinely brought to leadership's attention.

The *Caremark* decision was founded on a derivative suit filed against the board of a healthcare services company, claiming that the board neglected to exercise due care by failing to implement proper internal controls, which allowed its

employees to enter into illegal kickback schemes with referring physicians that resulted in the company paying more than \$250 million in fines and civil settlements. Chancellor Allen explained that the standard for oversight liability is that a "sustained or systematic failure" of the board to exercise oversight will create a lack of good faith, which is required to create a basis for director liability for corporate losses resulting from ignorance of legally violative activity. [6] The standard was intentionally, and notoriously, cast as one of the hardest theories a plaintiff could hope to win a judgment on, to avoid any liability on the part of the board for that which they had not prevented through good faith efforts at oversight.

Though often overshadowed by the good faith inquiry, the element of an oversight claim has its own meaning in IP loss cases. *Caremark's* case has followed the reasoning of the court in *Cede & Co v Technicolour Inc*, which was decided two years before *Caremark*, that "after the plaintiff establishes the existence of a fiduciary duty, the burden shifts to the defendant directors to prove that the transaction or decision was entirely fair." [6] This reasoning informed, but did not define, the causation analysis in oversight cases. [1] For a board defending an IP-loss oversight claim, this simply means that, once a plaintiff pleads particular facts to the effect that the board's IP reporting system was nonexistent or ineffective, the burden of showing that such a system would not have prevented the IP loss, or that the IP loss was not proximately caused by the failure [18] of the reporting system, is placed squarely on the board's shoulders, and it is costlier to prove that fact than it is to establish a reporting system in the first place.

2.2. The Caremark Doctrine and Its Modern Expansion (From Financial Controls to Operational/Cyber Risk)

The Delaware Supreme Court adopted the *Caremark* standard 10 years later in *Stone v Ritter* [18], which stated two questions must be answered: "Did the directors fail to implement any reporting or information system or controls?" or "Did the directors implement any reporting or information system or controls but choose not to monitor or oversee it so that they are not informed of risks or problems that might have been the object of their attention" [18] It was as if, for about two decades after *Caremark*, plaintiffs could not get a foot in the door of any jurisdiction to enforce the test, and commentators openly doubted whether *Caremark* liability actually existed, or whether it would be a real liability at all [40].

The Delaware Supreme Court, then headed by Chief Justice Stine, breathed new life into a *Caremark* claim in *Marchand v. Blue Bell Creameries* in March 2019, [13] in the wake of a listeria outbreak which resulted in the deaths of three people and a nationwide product recall, and required Blue Bell Creameries to enter into a dilutive private equity transaction to stay afloat. Despite the company's formality of regulatory compliance, the court stressed that food safety was the most

fundamental safety and legal compliance concern of a company making ice cream, and the board lacked a committee to monitor food safety, did not have a regular reporting process or protocol for the company to provide food-safety compliance information to the board, nor did the board have a schedule for considering food-safety concerns. [13] Three months later, the Court of Chancery agreed in *In re Clovis Oncology Inc Derivative* case that a board that received internal reports that contradicted the company's public statements concerning the efficacy of a cancer drug and failed to take any action after receiving those red flags might be liable for oversight failure even in the absence of a nominal monitoring system. [7] *In re Boeing Co. Derivative Litigation* (2021), the court applied this oversight framework to aviation safety. It denied a motion to dismiss, holding that the board's failure to rigorously exercise its oversight duties in a "mission-critical" operational area - specifically aircraft safety - directly caused the corporate breakdown [5, 47].

The most recent and important doctrinal innovation, and one that is most relevant to intangible-asset governance, is the Delaware Court of Chancery's January 2023 decision in *In re McDonald's Corp Stockholder Derivative Litigation*, in which, for the first time, the court determined that corporate officers, not just directors, have a fiduciary duty of oversight. [8, 50] The Officers were held to have more of these kinds of day-to-day interactions with the operational risks than the board itself, and that led the court to believe that they are subject to the same policies that would result in a duty to recognise an operational risk, [8, 39] even though the court emphasised that an officer's oversight responsibilities are usually narrower and limited to his or her own responsibility area, in contrast to a director whose duties are more comprehensive. [26] For the chief technology officer, chief information security officer, or general counsel who has the responsibility for intangible assets risk in their area of operation, *McDonald's* is a clear doctrinal warning: These officers now have an independent, personally enforceable oversight duty over their own domain in respect of the IP and cyber risk, a duty that recent scholarship on operational risk and outside compliance gatekeepers has independently confirmed [29].

2.3. Comparative Analysis: UK Companies Act (s.172/s.174) and Commonwealth Fiduciary Standards

By contrast, English law approaches corporate governance from a distinct jurisprudential tradition. Historically, directors' oversight and fiduciary obligations were governed primarily by common-law and equitable principles established through case law rather than a statutory code. While these rules were eventually codified under the Companies Act 2006 (notably Sections 171 to 177), English courts continue to interpret these statutory duties in light of traditional common-law precedents, maintaining a more flexible, case-by-case standard for director oversight.

Under this dual standard, a director must exercise the care, skill, and diligence expected of a reasonably diligent person carrying out those functions. This standard imposes a dual test: an objective floor, which establishes a baseline standard of competence expected of any director in that role, and a subjective ceiling, which elevates the required standard for directors who possess, or hold themselves out as having, special professional expertise. [20] The dual standard will have direct implications for non-executive directors who have been brought on to the board for their expertise in cybersecurity or intellectual property: Where the company incurs an "inevitable" loss of IP due to a cyber incident to which a competent IP specialist would have raised concerns, the non-executive director will be expected to adhere to a reasonable-IP-director standard.

The pre-2006 case law which informed the scope of permissible delegation remains of great value. For the Director, in *Re City Equitable Fire Insurance Co*, the Court of Appeal said that a Director was not required to keep close watch on the activities of the company and could, in the absence of any reason to suspect any wrongful activity, rely on the Directors' representative to carry out the duties in an honest manner, a concept which was expanded and now narrowed in *Re D'Jan of London Ltd*, where the Court held the Director liable for signing an insurance proposal form without reading it, saying that anyone who had any sense of duty would have done so. [14, 15] The Court of Appeal in *Lexi Holdings Plc (in Administration) v Luqman* [11] held that non-executive directors who in substance were totally inactive were in breach of their duty because directors have a continuing duty to obtain and maintain sufficient knowledge and understanding of the company's business to enable them to fulfil their duties, and that exercise of a power of delegation does not relieve or excuse any director from their duty to supervise the discharge of the delegated functions. The same rationale was used in *Madoff Securities International Ltd v Raven*, where it was held that a director's reliance on management's judgment, information and advice is limited by the ongoing supervisory obligation [12].

The principle which underlies the application of the earlier case of the Court of Appeal, *Re Westmid Packing Services Ltd*, is of the greatest importance: that any person who performs the statutory and fiduciary duties of a director will need to know that they are not merely a paper tiger, but that a "proper degree of stewardship" means that the individual director ought to be informed of the company's affairs and should be involved with other directors in the supervision and control of them. [16] This means that, when applied to a director who is not an executive director and has been appointed to a board based on his or her expertise in the technology, IP or cybersecurity field, that director is left in a materially weaker position to claim the protection of reasonable reliance than a director who is not knowledgeable in that field.

While the language used is slightly different, the practical application of both systems is still quite similar; both allow

the board or a director to delegate operational duties related to intellectual property to a specially designated officer; [20] and both systems remove the protection when the board or director is actually or constructively aware of the red flag, either because of a lack of a reporting system as Marchand has noted, or because of a lack of a duty to supervise delegated functions as Lexi Holdings has pointed out. [11] The board that fails to show a good working IP oversight system, or active oversight of the officers to whom IP risk has been delegated, is vulnerable on both sides of the Atlantic.

3. Modern IP Vulnerabilities as Corporate Governance Failures

3.1. Trade Secret Cyber-Theft and Industrial Espionage: Board Inaction as Breach of Duty

Waymo LLC v Uber Technologies Inc. is the classic case of the negative consequences of the negligence of boards and executives towards a well-known trade secret. Waymo claimed that it had more than 14,000 confidential files leaked by Anthony Levandowski, a former lead engineer on its self-driving car programme, after he quit to found a company Uber acquired for some \$680 m, and that Uber's own internal due-diligence report created before the deal closed identified that Levandowski was likely to have access to files with Waymo's own LiDAR technology. [51] It was noted that Uber's own internal due diligence report flagged that its acquisition target's co-founder was potentially in possession of some 14,000 files containing Waymo's proprietary information before the acquisition closed.

Nevertheless, Uber went ahead with the deal and verbally and in contract compensated Waymo against any claims for legal action brought on by the alleged infringement of the trade secrets, a move that, on the facts Waymo contended, seems more like a deliberate, upper management risk-taking without having taken board-level steps to assess and quantify what the exposure to the trade secrets is [54, 55].

After a gruelling discovery process, the Federal Circuit court decision required Uber to produce the entire due-diligence report, and a commitment that Uber would not use Waymo's confidential information in its autonomous vehicle hardware or software. The case was settled five days into the trial, with the parties agreeing to 0.34% of Uber's stock, valued at about \$245 million, along with a pledge that Waymo's confidential information would not be used in Uber's autonomous vehicle hardware or software. [54, 55] The case also led to another criminal referral: In another former Uber security officer's statement, the presiding judge said that the company's business of trying to acquire competitors' trade secrets was done in an "undue manner" [51].

The fallout from this case will not stop with the settlement;

internal evidence of theft of trade secrets and acquisition proceedings will continue to play out as the cornerstone of future trade secret cases between technology firms, as new plaintiffs and regulators have discovered and cited in other cases involving employee mobility between competitors, and as the old joke goes, a written report, if unexercised, is only a report. Trade secret theft carries a steep cost. For boards, the core governance lesson of *Waymo v. Uber* is that the risk was explicitly identified during due diligence, yet the acquiring party's deal team chose to proceed anyway. [30, 54] An effective board-level IP risk escalation mechanism, like Part 5 of this paper suggests, is precisely what prevents a red flag identified in due diligence from getting lost and neutralised at lower levels within the organisation where it would not be considered in making financing and governance decisions based on the strategic rationale of the acquisition. This is consistent with empirical evidence that firms make financing and governance decisions in response to IP risk rather than IP risk being a purely operational concern [23].

Regulatory oversight of cyber-related IP risk has evolved significantly since the *Waymo* settlement. A prime example is the SEC's landmark 2023 enforcement action against SolarWinds and its former CISO, Timothy Brown, following the Sunburst cyberattack - marking the first time a US securities regulator sought personal liability against a CISO over a public company's cybersecurity disclosures [43].

While the SEC may not have succeeded in its main arguments in July 2024, when the district court ruled that it had acted improperly in relying on hindsight and failed to prove that Brown intentionally failed to inform the executives involved in public disclosures of the company's cybersecurity shortcomings, leading to the dismissal of the case, it nevertheless concluded that a CISO's internal risk discussions are discoverable, and that internal dishonesty about unresolved cyber risks can blow back against the company if those risks are not escalated and addressed at the proper governance level [17]. *SolarWinds* shouldn't be interpreted as a triumph for boards that they would not have to worry about any cyber or IP vulnerabilities being exposed through internal reporting, [52] but rather as a cautionary tale about the evidentiary risk of having internal reporting on IP and cyber vulnerabilities that never reaches, or is not monitored by, the people responsible for the company's external representations [24].

3.2. Generative AI Deployment: Corporate Liability for Inadvertent IP Infringement and Data Loss

Generative AI introduces an IP risk never anticipated by *Caremark*: a company using its own technology to infringe on third-party IP rights due to improper training data. The scale of this exposure became clear in December 2023, when the New York Times sued OpenAI and Microsoft, seeking billions in damages and demanding the destruction of any models or datasets built on the newspaper's copyrighted content.

[19] In April 2025, a federal judge in New York denied the defendants' motion to dismiss the suit and allowed the essential direct and contributory copyright infringement claims to proceed, due to Microsoft's admission of many publicised instances of ChatGPT plagiarising material from the Times' articles. [19, 49] Whether it is a product or a productivity tool, for any board that trains, refines, or releases a large language model, *NYT v OpenAI* is now the key precedent that proves that the origin of the training data is more board-related than the technical or engineering aspects [27].

This paper offers a more complex governance lesson on the comparative UK position, which was enunciated in a decision only months before this paper was written. In *Getty Images (US) Inc v Stability AI Ltd* [2] the Court ruled in favour of a narrower aspect of Getty's trade mark claim: that early versions of the Stability AI model could create synthetic images with Getty's watermarks and against its broader copyright claim, which alleged that the model constituted an infringing "copy" of the millions of images used to train it, where the model was not stored or reproduced any of the underlying images [31].

Mrs Justice Smith's judgment explicitly recognised the delicate balance needed between creative rights and AI innovation. Yet, her mixed ruling offers no comfort to boards hoping generative AI deployment is a settled, low-risk domain. In fact, Getty's success on a claim its own lawyers considered secondary trademark infringement over synthesised watermarks - underscores that the legal landscape remains unpredictable and fraught with litigation risk. The board misread the *Getty* verdict by failing to recognise its narrow scope. The court's copyright findings turned on specific, quickly evolving model architecture, while the actual liability stemmed from an issue - watermark reproduction - that had received virtually no board-level attention before trial.

But whatever the outcome of both cases is, the implication for governance is the same: whether or not a deployed generative AI system will generate IP exposure for the operator is now a question that can only be solved by protracted litigation and multiple motions, and is a fact-based question, which is also technical in nature, rather than a legal sign-off question when the model is selected. [53] A board that approves the use of generative AI without a process to keep track of the provenance of the training data or to review its assessment as the underlying [53] model as the set of training data evolves is likely following the *Marchand* pattern [13] of assuming that a single point-in-time review is enough for a mission-critical and ongoing risk.

The heavy discovery burden in these cases illustrates why IP risk cannot be resolved through a single, pre-deployment legal opinion. [2] *The NYT v OpenAI* case has already triggered intense disputes over preserving billions of user conversations and generated high-stakes depositions of C-suite executives. Regardless of the ultimate verdict, this creates a multi-year evidentiary burden that strains corporate resources long

after technology deployment. [19] A board approving a Generative AI product without considering the possibility that later the product will be the subject of discovery for years to come without a clear documented record of the board's considered decision on the use of training data, whether that data is covered by licensing or fair-use restrictions and, if so, what the board did to decide that question, and by whom and when, is an evidentiary vacuum that will be filled by inference and reconstruction, if and when litigation occurs, without a clean, documented record of the board's decision.

3.3. Unmonitored Open-Source Integration and Risks to Proprietary Assets

Open-source software occupies a double-edged position in IP governance. While it offers software engineers significant development efficiency, it also introduces a massive, cumulative compliance risk that expands with every code commit. An analysis of more than 1,000 commercial codebase audits across 17 industries revealed that 84% of codebases contained at least one known open-source vulnerability, 74% contained high-risk vulnerabilities, and 53% contained open-source licence conflicts. [46] The Principles of Jacobsen [10] are a reaffirmation of the fundamental principles of US law on copyright licenses, namely that the specific conditions under which works are to be copied and modified under an open-source licence are conditions of the copyright licence itself, and not just contractual covenants which are breachable only in relation to damages. [10] The Federal Circuit held that the economic value open-source licensors derive from mandatory attribution and change tracking - such as driving traffic to their projects - is a legally protected interest. Copyright law does not merely regulate contracts; it exists specifically to safeguard and vindicate these economic and creative rights [10].

It is very easy to shrug off the governance importance of *Jacobsen* since compliance with open source is not likely to be a subject of discussion at the board level. [10] As opposed to a one-off licensing transaction that is legally reviewed at one point in time, the process of open-source integration is continuous and incremental, in which individual engineers take individual components of open source (libraries and packages) and integrate them into the company's shipping products, without necessarily having a centralised repository for which open-source licenses are used, or what license obligations are thus embedded. No company will know, and thus not be able to accurately inform IPO investors, licensees or regulators, how much of the company's IP is being exposed through the copyleft, if it has never done an enterprise-wide open-source bill-of-materials audit; and this oversight is even more significant when an acquisition occurs, when a company goes public, or when an enterprise licensing agreement is reached. [28, 46] The *Caremark* standard's requirement that a board must ensure that "a reasonable information and reporting system exists" literally comes down to this: If a board never asks if such a system exists, then it has never tried to

establish an oversight role over one of the most important and continuously operating sources of IP risk that a software-dependent company has [13].

The extent of this exposure is quantifiable, yet deeply troubling. The Synopsys Cybersecurity Research Centre's 2024 Open-Source Security and Risk Analysis Report revealed that over 53% of audited codebases contained license conflicts - the exact type of non-compliance that *Jacobsen* establishes as grounds for copyright infringement claims. Concurrently, high-risk vulnerabilities surged from 48% in 2023 to 74%. [46] As *Marchand* establishes, a board breaches its fiduciary duties simply by failing to monitor its exposure to license conflicts relative to industry baselines. This failure of oversight exists independent of harm; the breach occurs regardless of whether a dispute ever materialises into tangible loss.

4. The Business Judgment Rule and IP Risk Management

4.1. Distinguishing Reasonable Business Risk from Uninformed Fiduciary Failure

The Delaware court did not second-guess a decision made by directors on an informed, good-faith, and honest belief that the action taken was in the best interests of the company, and the business judgment rule assumes that the directors made their decision on an informed basis, in good faith and in honest belief that the action taken was in the best interests of the company. [1] The Delaware Supreme Court's ruling in *In re Walt Disney Co Derivative Litigation* [9] however, has made it clear that a board which approves a major transaction, in the instant case, an executive severance agreement, without adequate information or deliberation waives the protection of the rule, even if the underlying substantive decision might otherwise have been sound. In terms of IP risk, a board that has asked and decided to tolerate a certain amount of risk of losing its trade secret, AI training data, or open source is shielded by the rule. In contrast, a board that did not ask questions is open to oversight liability whether or not the underlying business decision was reasonable.

This difference holds especially true in the generative AI realm, where technological evolution can make an informed decision challenging. [2, 32] Although a board does not have to be as technologically sophisticated as a machine-learning engineer to satisfy the *Caremark* rule, it does not require it to duplicate the function of specialised management; rather, it is enough that a board affords itself protection by ensuring that a reasonable reporting and escalation process exists, by which management's specialised assessment makes its way to the board when the underlying risk is material. [4] A board that has already, and regularly, replaced with a documented assessment the legal exposures and provenance of the company's training data for generative AI has fulfilled its oversight duty, even if the final legal analysis turned out to have understated

a rapidly evolving legal exposure; a board that failed to commit to a documented assessment of the company's training data for generative AI, at least, has not.

A line between protected business judgment and unprotected uninformed failure is therefore not one between cautious and aggressive IP strategies; a board may reasonably choose to take a lot of risk for AI training data to get the first-mover advantage, [10] or a board may be more willing to accept a certain amount of uncertainty around the open-source licence in exchange for the engineering velocity, and either decision is within the protected scope of the business judgment rule as long as it was actually made, and not made. [38, 39] However, the "*fiduciary question*" that boards should be considering is not whether they have a high or low tolerance for IP risk, but whether that tolerance has been subjected to a board-level vote, in contrast to a "default" outcome whereby no one ever asked the question, which is consistent with the new mission-critical-risk framework that *Caremark* scholarship has evolved, to this point [1].

4.2. Establishing Reasonable Board Oversight: IP Audits, Reporting Systems, and Escalation Protocols

The six principles for cyber-care oversight that are defined in the National Association of Corporate Directors (NACD) and Internet Security Alliance's 2023 Director's Handbook on Cyber-Risk Oversight are adapted with only minor changes to become principles for IP risk oversight, and are used on four levels: Directors should view the risk as a board-level, enterprise-wide risk instead of a technical risk; Directors should be familiar with the legal implications of the risk on the company's specific business; Directors should ensure that management has in place a board-level, enterprise-wide risk management program with sufficient staffing and budget; and, Directors should engage in board deliberations to understand the financial exposure, and decide which risks are to be accepted, mitigated, or transferred. Principle six of the updated 2023 edition also requires Directors to encourage systemic resilience by collaborating with industry and governmental peers. [43, 48] The Handbook's focus on quantification is easily applicable to IP risk: A board that actively evaluates its exposure to trade secret theft, AI training litigation, or open-source non-compliance creates a record protected by the business judgment rule. Conversely, a board that fails to evaluate these risks abdicates its oversight role and forfeits that legal protection.

There are three interrelated pieces that need to be part of a working IP oversight system. First, there must exist a standing IP and technology risk inventory which must be updated continuously - not merely triggered by transactions or disputes. This inventory should track access controls over the existing trade secret portfolio, map the provenance of training data, and monitor open-source licensing obligations across the company's current codebase. Second, risks identified should not be resolved at the operational level but reported to the

board or a delegated committee when they reach a threshold rather than closing them at their identified level, as this may suggest that there is risk identification threshold at all. [41, 43] Third, there must be a fixed reporting cycle modeled on audit committee standards. Receiving information only when a crisis erupts rather than on a regular, structured schedule was precisely what spelled the death knell for the board's defense in *Marchand* [13].

In the IP context, the Handbook's recommendation that boards adopt defensible risk-quantification methods is especially critical. Unlike data breach notifications - where costs can be readily estimated using historical claims data - calculating IP risk and intangible asset exposure is far more complex and nuanced. [48] The cost of a trade secret portfolio, the threat of an AI training corpus that turns out to be open source licensed with competing claims, and the cost of remediation of the open source conflict that is uncovered after deployment are all real challenges that require board evaluation [37].

4.3. The Role of Director & Officer (D&O) Insurance in Intangible Asset Protection

While director and officer liability insurance and IP oversight risk are often linked, boards do not always know how this insurance works until a claim is made. [17, 35] As a result of the McDonald's litigation, insurers came to reconsider how to price and cover a director's exposure to the Caremark liability, as this oversight risk had not previously been treated as a standard component of traditional officer exposure. The *McDonald's* decision marked a critical turning point for the D&O insurance market. In its wake, underwriters fundamentally re-examined how they priced and structured *Caremark* coverage - with some insurers explicitly excluding oversight exposure on the grounds that it departed from traditional risk models [8].

These coverage disputes are especially common in the IP realm because most D&O and cyber-insurance policies were designed for traditional data breaches and unauthorized personal data access. They were not structured to address emerging risks like AI training-data infringement or trade secret disputes arising from employee mobility. A board that fails to evaluate whether its policy explicitly covers these modern IP liabilities risks facing devastating coverage denials when a claim is made [17].

Another challenge is that insurers are increasingly asking for proof of the governance structure, IP risk inventory, escalation protocol, and documented AI governance amongst other things, as underwriting conditions; this is similar to the underwriting conditions for cyber-insurance, which requires adherence to standards of information-security management, such as ISO/IEC 27001, [22] as a prerequisite for coverage or as a factor that influences premium. The practical implications are that boards have two additional commercial motives, beyond the fiduciary duty, to formalise IP oversight: it is a condition-precedent for securing or maintaining IP-related insurance cov-

erage on reasonable terms, and second, it provides an independent commercial reason for a board to formalise IP oversight rather than leave it within the informal network of engineering and legal responsibilities [30].

Boards must scrutinize - rather than assume - the geographic scope and specific claim types covered by their insurance policies. A policy negotiated primarily to mitigate U.S. litigation exposure may fail to respond effectively to UK proceedings like *Getty Images v. Stability AI*. This is particularly true given the UK's narrower statutory framework for secondary copyright infringement in AI models and its distinct legal standards for trademark infringement. [2] The lesson, in practice, is that the IP oversight committee suggested in Part 5 of this paper should not be sitting on a coverage summary that the company prepared only when the policy was placed but hasn't reviewed since, but instead review the company's D&O and IP-specific coverage on an annual basis based on the jurisdictions in which the company is exposed to AI, trade secret and open-source claims.

5. A Proactive Legal Framework for Board-Level IP Oversight

5.1. Guidelines for Board Charter Revisions and IP Oversight Protocols

A key first step to establishing a defensible IP oversight structure is an amendment to the board charter that expressly identifies both IP and technology risk as an audit committee or board's duty. [43] Because *McDonald* confirms that an officer's silence in the face of a red flag in that officer's area of specialisation is sufficient to trigger the obligation to make a report, it is equally important that the charter or an accompanying delegation resolution prescribe who has front-line responsibility for each category of IP risks. [8] The charter should also include a regularity of reporting to the board on IP risks; the types of incidents that should be escalated immediately as opposed to on a regular basis, based on the categories of incidents covered in Part 3; and the board's expectation that management will keep the rolling inventory of risks [43].

Delaware's exculpation statute allows corporations to eliminate director liability for breaches of the duty of care, but it explicitly excludes the duty of loyalty. Because *Caremark* oversight liability is anchored in the duty of loyalty - requiring a showing of bad faith rather than mere negligence - exculpation provisions offer directors no shield against oversight claims. [21] This means that with a properly pleaded claim in IP oversight, exculpation clauses, no matter how broadly drafted, do not shield directors from liability, and in fact do not limit the impact of the changes to the charter and protocol proposed here: Directors are not excused from liability for failing to have a workable IP reporting system simply by including broad exculpation clauses in their charter.

5.2. Governance Best Practices for Directors: Escalation Trees, Routine IP Valuations, and Vulnerability Audits

The escalation tree for IP risk should reflect the escalation paths and response timelines that have been successful in safety and cybersecurity situations outlined above: a defined subset of events that trigger escalation; each escalation tied to a specific response timeline and a particular escalation path, not left to the judgement of the next manager in the chain. Periodic board level valuation exercises, like those performed by the *Ocean Tomo* intangible asset market, and value methodology at the market level, complement each other: [45] a board that periodically reviews the estimated value of its trade secret portfolio, patent estate, and proprietary data is better equipped to ensure that they are being protected than a board that does not know what they are worth. [45] Vulnerability reviews, which are more common than in a stable patent portfolio and are performed at regular intervals that correspond to the risk inventory's change, complete the cycle of the risk inventory,

This standard applies with particular force to non-executive and independent directors. A stark illustration of bad practice emerged in *Re Lexi Holdings Plc* [11], where a non-executive director ignored a fictitious loan account appearing in the corporate books - failing to read, question, or take any action regarding the financial anomaly. Merely reviewing a report before presenting it to the board does not discharge a director's fiduciary duty if they fail to read it prior to formal execution. Under the principle established in *Re D'Jan of London Ltd*, a director who signs off on an IP risk report without first reading and understanding its contents breaches their duty of care.

6. Conclusion

Option 1: Direct & Polished (Recommended)

The jurisprudence traced in this paper - from *Graham's* restrictive bad-faith test, through *Caremark's* demanding yet largely theoretical oversight standard, to the recent revival of oversight duties triggered by absent reporting systems and extended to corporate officers - reflects a driven evolution of what good-faith governance requires of a modern board. To date, this judicial recalibration has occurred almost exclusively in response to physical safety crises, financial fraud, and workplace misconduct. What has yet to materialize before the courts is an IP oversight failure - a case where a board completely abdicates its duty to monitor intangible assets. Yet the doctrinal architecture is already established, and five decades of *Ocean Tomo* data prove that the underlying commercial exposures are now fully in play: In the *Marchand* case IP risk arena, an unmonitored trade secret exposure was discovered during due diligence, only to be ignored; In the *Caremark* case, an open-source compliance failure was uncovered only during an acquisition due diligence; and, In the generative AI

arena, facts that an unchecked trade secret exposure was documented in due diligence and ignored, and facts that a generative AI system was trained without a documented provenance review, were all in play.

This paper serves as an urgent warning: boards must not wait for a court to decide this test case against them. Establishing IP risk oversight is not a discretionary best-practice add-on - it is the direct application of existing *Caremark* doctrine. Boards bear an unyielding duty to maintain reasonable information and reporting systems for risks central to the corporate enterprise. Given that intangible assets now comprise the vast majority of enterprise value, a board that would never tolerate the absence of financial controls or safety oversight - as seen in *Marchand* - has no legal or commercial justification for failing to establish oversight systems for the very assets that define its market worth.

Abbreviations

IP	Intellectual Property
AI	Artificial Intelligence
CISO	Chief Information Security Officer
SEC	U.S. Securities and Exchange Commission
NACD	National Association of Corporate Directors
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission

Author Contributions

Oduyebo Tomilayo Olubisi: Conceptualization, Methodology, Resources, Writing – original draft, Writing – review & editing

Akinsola Oluwaseun Kayode: Resources, Supervision, Writing – review & editing

Agboke Mutiu: Resources

Adetoye Funmilola Abeke: Resources

Conflicts of Interest

The authors declare no conflicts of interest.

References

- [1] *Cede & Co v Technicolor Inc*, 636 A. 2d 956 (Del 1994).
- [2] *Getty Images (US) Inc and others v Stability AI Ltd* [2025] EWHC 2863 (Ch).
- [3] *Graham v Allis-Chalmers Manufacturing Co*, 188 A. 2d 125 (Del 1963).
- [4] *Guttman v Huang*, 823 A. 2d 492 (Del Ch 2003).
- [5] *In re Boeing Co Derivative Litigation*, 2021 WL 4059934 (Del Ch, 7 September 2021).

- [6] *In re Caremark International Inc Derivative Litigation*, 698 A. 2d 959 (Del Ch 1996).
- [7] *In re Clovis Oncology Inc Derivative Litigation*, 2019 WL 4850188 (Del Ch, 1 October 2019).
- [8] *In re McDonald's Corp Stockholder Derivative Litigation*, 291 A. 3d 652 (Del Ch 2023).
- [9] *In re Walt Disney Co Derivative Litigation*, 906 A. 2d 27 (Del 2006).
- [10] *Jacobsen v Katzer*, 535 F3d 1373 (Fed Cir 2008).
- [11] *Lexi Holdings plc (in administration) v Luqman* [2009] EWCA Civ 117.
- [12] *Madoff Securities International Ltd (in liquidation) v Raven* [2013] EWHC 3147 (Comm).
- [13] *Marchand v Barnhill*, 212 A. 3d 805 (Del 2019).
- [14] *Re City Equitable Fire Insurance Co* [1925] Ch 407 (CA).
- [15] *Re D'Jan of London Ltd* [1994] 1 BCLC 561 (Ch).
- [16] *Re Westmid Packing Services Ltd* [1998] 2 BCLC 646 (CA).
- [17] *Securities and Exchange Commission v SolarWinds Corp and Timothy G Brown*, No 1: 23-cv-09518-PAE (SDNY, 18 July 2024).
- [18] *Stone v Ritter*, 911 A. 2d 362 (Del 2006).
- [19] *The New York Times Company v Microsoft Corporation*, No 1: 23-cv-11195 (SDNY).
- [20] *Companies Act 2006* (UK).
- [21] *Delaware General Corporation Law*, tit 8.
- [22] *ISO/IEC, ISO/IEC 27001: 2022 Information Security, Cybersecurity and Privacy Protection* (ISO 2022).
- [23] Ionela Andreicovici, Sara Bormann and Katharina Hombach, 'Trade Secret Protection and the Integration of Information Within Firms' (2025) 71(2) *Management Science* 1213-1237. <https://doi.org/10.1287/mnsc.2021.03484>
- [24] Jennifer Arlen, 'Directors' Caremark Liability for Fraudulent Disclosures to Customers about the Company's Cybersecurity: SolarWinds Reconsidered' (2025) 50 *Journal of Corporation Law* 1107.
- [25] Emanuel Bagna, Enrico Cotta Ramusino, Stefano Denicolai and Roger Strange, 'Intangible Assets and Firm Performance: The Relative Effects of Recognized and Unrecognized Assets' (2024) 10(3) *Journal of Open Innovation: Technology, Market, and Complexity* 100356. <https://doi.org/10.1016/j.joitmc.2024.100356>
- [26] Robert C Bird and Julie Manning Magid, "Operational Risk and the New Caremark Liability for Boards of Directors" (2023) 103 *Boston University Law Review* 1539.
- [27] Adam Buick, 'Copyright and AI Training Data Transparency to the Rescue?' (2025) 20(3) *Journal of Intellectual Property Law & Practice* 182-192. <https://doi.org/10.1093/jiplp/jpae102>
- [28] Felix Kwabena Danso, Michael Adusei, Beatrice Sarpong-Danquah and Kwadwo Boateng Prempeh, 'Board Expertise Diversity and Firm Performance in Sub-Saharan Africa: Do Firm Age and Size Matter?' (2024) 10 *Future Business Journal* 98. <https://doi.org/10.1186/s43093-024-00386-6>
- [29] Asaf Eckstein and Roy Shapira, "Compliance Gatekeepers" (2024) 41 *Yale Journal on Regulation* 469.
- [30] Scott Guernsey, Kose John and Lubomir P Litov, "Actively Keeping Secrets from Creditors: Evidence from the Uniform Trade Secrets Act" (2022) 57(7) *Journal of Financial and Quantitative Analysis* 2516-2558. <https://doi.org/10.1017/S0022109022000084>
- [31] James Hall, 'Why Getty Images v Stability AI Got Secondary Copyright Infringement Wrong' (2026) *Journal of Intellectual Property Law & Practice* (advance article, jpag074). <https://doi.org/10.1093/jiplp/jpag074>
- [32] Geneviève Helleringer and Florian Möslin, 'AI & the Business Judgment Rule: Heightened Information Duty' (2023) *University of Chicago Law Review Online*.
- [33] Claire A Hill and Zohreh Zakiani, 'What Should Caremark Encompass?' (2024) 19 *Brooklyn Journal of Corporate, Financial & Commercial Law* 33.
- [34] Panern Intara and Nittikorn Suwansin, 'Intangible Assets, Firm Value, and Performance: Does Intangible-Intensive Matter?' (2024) 12(1) *Cogent Economics & Finance* 2375341. <https://doi.org/10.1080/23322039.2024.2375341>
- [35] WeiWei Li, Prasad Padmanabhan and Chia-Hsing Huang, 'Directors' & Officers' Liability Insurance and Financing Decisions: Evidence from Debt Structure Choice' (2024) 83 *Pacific-Basin Finance Journal* 102248. <https://doi.org/10.1016/j.pacfin.2023.102248>
- [36] Michelle R Lowry, Anthony Vance and Marshall D Vance, 'Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity' (2026) 72(2) *Management Science* 783-804. <https://doi.org/10.1287/mnsc.2023.04147>
- [37] Camélia Radu and Nadia Smaili, 'Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure' (2022) 177(2) *Journal of Business Ethics* 351. <https://doi.org/10.1007/s10551-020-04717-9>
- [38] Roy Shapira, "A New Caremark Era: Causes and Consequences" (2021) 98 *Washington University Law Review* 1857.
- [39] Roy Shapira, "Mission Critical ESG and the Scope of Director Oversight Duties" (2022) *Columbia Business Law Review* 732.
- [40] Yehonatan Shiman, 'The Politics of Oversight: Caremark, Corporate Purpose, and Delaware's Judicial Landscape' (2025) 62 *American Business Law Journal* 165.
- [41] Nadia Smaili, Camélia Radu and Amir Khalili, 'Board Effectiveness and Cybersecurity Disclosure' (2023) 27(4) *Journal of Management and Governance* 1049-1071. <https://doi.org/10.1007/s10997-022-09637-6>

- [42] Serdar Turedi and Asligul Erkan-Barlow, 'CIO Equity Compensation and IT Investment: The Moderating Role of Board Monitoring and Evidence of Managerial Myopia' (2023) 15(6) *Review of Behavioral Finance* 916.
<https://doi.org/10.1108/rbf-04-2022-0118>
- [43] National Association of Corporate Directors and Internet Security Alliance, 2023 *Director's Handbook on Cyber-Risk Oversight*.
- [44] Ocean Tomo, "Ocean Tomo Releases Intangible Asset Market Value Study Interim Results for 2020" (Ocean Tomo, 22 September 2020).
- [45] Ocean Tomo, "Ocean Tomo Releases 2025 Intangible Asset Market Value Study Results" (J. S. Held, 12 February 2026).
- [46] Synopsys Cybersecurity Research Centre, 2024 *Open-Source Security and Risk Analysis Report* (Synopsys, 27 February 2024).
- [47] "Boards' Duty of Oversight: From Caremark to the Continuing Travails of Boeing" American Bar Association, *Business Law Today* (13 May 2024).
- [48] "NACD Director's Handbook Builds Support for Cyber Risk Quantification" (FAIR Institute, 28 March 2023).
- [49] "New York Times vs. OpenAI Lawsuit Status and Timeline" (Legal Clarity, 18 June 2026).
- [50] "Recent Delaware Cases Clarify Caremark Oversight Duties for Directors and Executive Officers" (Bryan Cave Leighton Paisner, 25 April 2023).
- [51] "Shedding Some Light on a Shady Business: Waymo and Uber Face Off in LiDAR Trade Secret Case" *North Carolina Journal of Law & Technology* (blog, 2018).
- [52] "SolarWinds Dismissed: What the SEC's U-Turn Signals for Cyber Enforcement" *Harvard Law School Forum on Corporate Governance* (7 December 2025).
- [53] "Stability AI Defeats Getty Images Copyright Claims in First of Its Kind Dispute Before the High Court" (Bird & Bird, November 2025).
- [54] "Uber, Waymo Reach Surprise \$245M Settlement in Trade Secrets Case" *NBC News* (9 February 2018).
- [55] "Waymo v. Uber 'Epic' Trade Secret Case Involving Autonomous Vehicles Settles for \$244 Million" (Butzel Long, 2018).