International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

The Speak-Up Dividend: Mitigating the Catastrophic Costs of Silence Through Structural Neutrality and Leadership Accountability

Vanshika Jain[a]

[a]Teerthanker Mahaveer University, Moradabad, India

Received 05 May 2026; Accepted 04 June 2026; Published 08 June 2026

The contemporary corporate governance system has experienced great change, moving away from rigid top-down institutional hierarchies to decentralised, proactive internal structures in which whistleblowing is a key component of ethical corporate practices. The paper provides a detailed comparative study of whistleblowing frameworks worldwide, comparing the United States' incentive-based bounty program, the European Union's multi-tiered structure, and the emerging statutory frameworks and actual compliance gaps of many developing nations, including India. Additionally, this paper assesses the potential of ISO 37002 and modern digital reporting tools to transform the disclosure ecosystem. This study, using Moral Judgment Theory and Power Dependence Theory, explores the moral and ethical processes that lead to the silence or disclosure of employees. It also analyses qualitative case studies of the three largest corporate failures in history: Enron, Wells Fargo, and Volkswagen. These institutionalised cultures of silence have negatively affected these companies and their shareholders' financial and reputational wealth. Through analysis, there is an indication that the formalised existence of an anti-retaliation policy is not sufficient. In addition to the statutory mechanisms available, there are significant gaps in implementation driven primarily by the pervasive nature of intimidation within the organisational culture, a lack of genuine anonymity in reporting and pronounced fears of occupational retaliation that discourage employees from utilising their rights under the statutory anti-retaliation provisions. This analysis identifies that an organisation

must have structural neutrality of independent operational bodies to facilitate the creation of a foundation of 'psychological safety.' As ESG reporting continues to increase in complexity and Artificial Intelligence deployment presents unprecedented risk, proactive governance will become essential. Therefore, this analysis recommends implementing a tripartite strategic model (leadership accountability, psychological safety and strong internal reporting mechanisms), which could successfully transform the act of whistleblowing into a proactive strategy.

Keywords: *corporate governance, whistleblowing, psychological safety, fear of retaliation, ethics premium.*

INTRODUCTION

Corporate Governance has changed significantly over time. Corporate Governance is no longer a 'top-down' hierarchy but instead is decentralised, vigilant, and involves internal reporting governance. Whistle-blowing was once seen as a rebellious act against authority or a sign of disloyalty. Today, it is accepted as one of the most effective ways to prevent fraud and corruption and reduce systemic risk. The evolution of whistle-blowing has been validated by a complex and developing pattern of International Law voluntary standards set by managers and the rapid expansion of technology to help individuals maintain their privacy. The effectiveness of Whistle-blower Protection Programmes is now considered an indicator of an Organisation's ethical development, operational viability, and long-term sustainability, by the Regulations, Investors, and the general public.

There are numerous Whistle-blower Protection Laws in many countries. A high number of countries have adopted some form of Whistle-blowers Protection Laws through a series of bilateral agreements between nations. Different Countries had different philosophies regarding Corporate Accountability. As such, laws differ from country to country, depending on each country's philosophy. The countries that represent each of those varying philosophies are the United States, the United Kingdom, the European Union, and India. Each of these countries provides a different type of protection to whistleblowers, and all of them also provide different types of incentives and obligations that come from reporting corporate violations.

United States (US) Model: The U.S. has arguably the most intricate, monetary-based whistleblower systems on the globe. SOX (2002) and Dodd-Frank Act (2010)[1] are at the centre

[1] Dodd-Frank Wall Street Reform and Consumer Protection Act 2010

of that system. Two significant legislative initiatives in the United States, the Sarbanes-Oxley Act (SOX)[2] and the Dodd-Frank Act, have reshaped the U.S.'s robust whistleblower protection laws. SOX was passed in response to the Enron-WorldCom debacle, and it targeted corporate auditing failures that led to a collapse in public trust in investors. It requires all public companies to maintain a means for employees to report concerns regarding auditing or accounting irregularities anonymously. SOX Section 806 prohibits public companies and their subsidiaries from retaliating against an employee who reports to a federal agency, Congress, or internal supervisors for securities fraud, mail fraud, wire fraud or bank fraud. Under SOX, any employee who has a reasonable basis for believing that a violation of securities law has occurred cannot be discharged, discriminated against or otherwise dissuaded from reporting the incident. In Lawson v FMR[3], the judicial ruling helped to clarify that Section 806 protections also apply to employees of contractors and subcontractors of a public company, ensuring that the 'arms-length' concept does not somehow create a vacuum of responsibility in the company. The Dodd-Frank Act establishes a more extensive bounty program under the SEC/CFTC, providing for whistleblowers who provide original information leading to enforcement action by federal regulators for a violation of federal securities and commodities law, and where the resulting penalties exceed $1 million. The Dodd-Frank Act also provides additional protections and payment of a bounty from 10% to 30%, based on the total penalty amount collected, to a whistleblower who provides the SEC with original information related to a securities law violation. The maximum bounty that can be paid to the whistleblower will equal 10-30% of the total amount of any monetary penalty greater than $1 million that has been levied against a party who is responsible for the violation being reported. These incentivised high-level disclosures have resulted in billions of dollars recovered. One of the most important developments regarding the evolution of the Dodd-Frank Act occurred with the Supreme Court decision in Digital Realty Trust[4], Inc. v Somers, which held that the Dodd-Frank Act's anti-retaliation protections only apply when an individual reports an alleged violation to the SEC directly. Because many companies have internal reporting policies encouraging employees to report misconduct internally, this creates a dilemma and a challenge for companies) For whistleblowers that reports internally may not be protected by Dodd-Frank's federal anti-retaliation protections unless they

[2] Sarbanes-Oxley Act of 2002
[3] *Lawson v FMR LLC* [2014] 571 US 429
[4] *Digital Realty Trust, Inc v Somers* [2018] 138 S Ct 767

also report to an outside agency, as this may lead to increased incentives for employees to report externally.

European Union (EU) Model: The EU's common minimum standards directive is based on a 'three-tier model' of reporting and covers all sectors and types of misconduct. All private sector companies with more than 50 employees and all public sector companies are required by the EU to have formal internal reporting mechanisms. This contrasts with the fragmented reporting requirements of the U.S. model based on the type of fraud. The new European Union Directive puts in place a complete reporting structure to report EU law violations in different categories, including public procurement, financial services, product safety, environmental protection, and data protection law violations. The multi-tiered approach of the EU provides an opportunity for the employee to report any wrongdoing internally within the workplace, thereby allowing the employer a chance to try to correct the matter before reporting it to the public or notifying the appropriate regulatory body. However, an employee will have the ability to report externally to a regulatory body if there is no resolution to the employee's internal report, or if the employee believes his employer will retaliate against him for making an outside report or destroying evidence of the wrongdoing. The EU is making strides to adopt a 'bounty' system for reporting; however, the EU has been very slow to endorse such a system due to prevalent cultural beliefs that support malicious and opportunistic reporting. However, each individual member nation has the ability to create its own bounty-type procedure in its own jurisdiction.[5]

United Kingdom (UK) and Emerging Economies: The United Kingdom's Employment Rights Act[6] is a law that protects employees who make disclosures with respect to impropriety against the public interest, including criminal acts, breaches of legal obligation, and health & safety threats. The UK continues to align itself with many of the EU-established standards following the exit of the UK from the EU. However, the UK's legal framework is already broader than the U.S. Sarbanes-Oxley Act of 2002. Likewise, many of the emerging economies do not have sufficient mechanisms or cultural commitment to support disclosure; therefore, employees working for organisations operating in many emerging economies are at significantly greater

[5] Protection of Persons who Report Breaches of Union law 2019
[6] Employment Rights Act 1996

risks of retaliation, even in those countries where there are written policies that provide for whistleblower protection.

India's Evolution of Whistle-blowing from Customary to Statutory System: The introduction of whistleblower programs in India was the result of the enactment of the Companies Act[7] and the regulatory requirements established by the Securities and Exchange Board of India for publicly traded companies to implement a 'vigil mechanism'[8] to allow employees or directors to voice concerns about inappropriate conduct, instances of fraud, or violations of a company's code of conduct. However, despite having a legal framework for whistleblower protection under the Companies Act and the SEBI regulations, there is a significant gap between how companies comply with the regulatory requirements and how well the policies are implemented in companies' cultures in India. An assessment of 100 major listed companies in India revealed that 94% of companies had policies with anti-retaliation provisions, but only 35% of those companies communicated the policy to their employees. Furthermore, approximately 54% of companies do not permit anonymous reporting, requiring a whistleblower to identify themselves before an investigation can occur; therefore, this provision creates an impediment in a corporate culture with significantly high levels of fear of retaliation. Whistleblowing Management Systems (ISO 37002 & Reporting Mechanisms) Building a culture of trust that promotes employee reporting requires more than just having a suggestion box; it requires a comprehensive program including multiple reporting channels, strict procedures for confidentiality, and clear accountability. Organisations must utilise the methods for reporting data that are appropriate for their size, workforce characteristics and cultural objectives.

ISO 37002: STANDARDISING WHISTLEBLOWING MANAGEMENT SYSTEMS

The publication of the ISO 37002:2021 standard marks a significant turning point in the standardisation of behaviour related to corporate ethics. As the first international consensus framework for Whistleblowing Management Systems (WBMS), it establishes a blueprint for organisations to develop a 'speak up' culture based on the principles of trust, impartiality, and protection. ISO 37002 uses the PDCA method for its appearance, and uses whistleblowing in all of its activities, in all of its experiences, not just as an administrative process, and changes to be

[7] Companies Act 2013
[8] Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015

made to better manage whistleblowers as noted in the plan. This plan sets out how to handle a report by assessing whether it falls within the definition of a 'wrongdoing' provided in the plan; how much this assessment satisfies the definition of a 'wrongdoing'; who will conduct the assessment; and to what extent the assessment will satisfy the definition of a 'wrongdoing'. The organisation's procedures outline what constitutes a 'wrongdoing', which determines which acts of wrongdoing can be reported through a whistleblower or employee reporting system, and where the report will be sent. Whistleblowers must be treated fairly; therefore, a Whistleblower Management System (WBMS) has been established to provide systems to evaluate reports or complaints made by the whistleblower. Whistleblower support and protection examples include providing emotional assistance to the whistleblower, providing modifications to the work environment of the whistleblower, helping the whistleblower alleviate feelings of guilt or shame, and creating plans for the safety of the whistleblower. Once the reports have been assessed, there will either be a completion of the report, or it will be sent to the proper persons for further investigation, if needed. To ensure that the WBMS remains in compliance with ISO 37002, every year or every few years, a WBMS must evaluate in terms of quantifiable metrics the number of reports that have been received, the average time it took to be resolved, and feedback from employees on how much they trust the WBMS is working, and to identify deficiencies to improve the WBMS. The ten core capabilities outlined within ISO 37002's WBMS will guide a company's complete process from the creation of initial policy to the ability for the company to, after having received reports of wrongdoing from employees, improve and implement any changes to its policies or procedures necessary to comply with the requirements.

DIGITAL REPORTING APPLICATIONS AND ARTIFICIAL INTELLIGENCE

Modern organisations are leaving behind traditional approaches to reporting, like lengthy 'paper trails or paperwork', in favour of more streamlined approaches, interactive dialogue-based reporting to enhance the whistleblower's experience with the reporting process. For example, there are platforms available today from leading vendors, which offer the following functionality to reduce barriers of entry for whistleblowers to utilise the reporting channels that are made available to them:

24/7 Hotlines and Live Agents: Reporting through a human-centred reporting experience to any place in the world in over 150+ languages to ensure workers do not miss opportunities to report impropriety due to time zones and/or language barriers.

Anonymity and Encryption: Well-designed technology platforms use very advanced end-to-end encryption with anonymity to provide whistleblowers the necessary security, confidence and trust to report impropriety.

An Organisational Ombudsman (OO) has an essential yet frequently unacknowledged function in conflict-resolution and risk-reduction processes within organisations. The OO is an experienced, independent, and unbiased professional who is well-versed in both conflict-resolution and risk-reduction methodologies. OOs adhere to four core principles established by the International Ombuds Association[9] (IOA) Standards of Practice.

The OO reports directly to the highest level of the organisation and is uninfluenced by any part of the organisation, including human resources and legal departments. OOs have no affiliation with nor advocate for any individual, and instead advocate for fair processes and outcomes. There is a strict maintenance of confidentiality by an OO, and no one can require an OO to disclose the identity of an OO's visitors. Therefore, an OO provides a 'haven' for employees to discuss options relating to their concerns without running the risk of formal actions occurring prior to adequate analysis and discussion of the concern with the OO. It does not provide binding decisions or participate in formal investigations. Instead, OOs primarily utilise 'shuttle diplomacy', as well as informal mediations, to assist constituents with resolving issues before they escalate into substantive formal disputes. Together, OOs are an important 'early detection diagnosis system' by identifying patterns of recurring behaviours or systemic deficiencies, while preserving the anonymity of individuals. They also assist constituents with navigating through the organisation's 'Conflict Management System' to select the best means to address their respective concern.

IMPLEMENTATION IN OPERATIONS: TIME FROM THE POINT TO RESOLUTION

Moving from a theoretical policy to an operational way of implementing that policy has to be done in a disciplined manner related to the 'life cycle' of a whistleblower report. Every stage of

[9] *IOA Standards of Practice* (International Ombuds Association, 2009)

the life cycle has the potential to experience failures that can erode trust and create significant legal and reputational risk to the entity, including a confusing intake form or a biased investigation.

Intake Phase: Designing the Entry Point to be Accessible: The intake portion of the whistleblower process is the most critical point in the overall whistleblower policy. Put into practice at the intake stage using best practices, companies/organisations develop two or more different report channels. The reporting channels should not be connected to the normal chain of command, as they need to be independent of the normal management hierarchy in order to exist free of conflicts of interest potentially arising among middle management, i.e. the primary source of wrongdoing. Effective intake forms are designed to gather quality information related to alleged wrongdoing, but they do not impose an unreasonable burden upon the reporter. OSHA and other types of organisations, a sophisticated corporate entity, have developed a methodology that involves no-cost translation services and the inclusion of open-ended questions within the intake form to allow the lowest-level or most vulnerable employee to utilise the intake system. In the 'California model' for intakes, employees in the process of reporting alleged wrongdoing are actively engaged in the process, and the reported alleged wrongdoing has the potential for a widespread impact on the industry.

Triage and Assessment Phase: Most organisations receive more reports than they have resources to appropriately investigate, and a structured triage process is necessary. Reports should be categorised by type of larceny, unsafe work condition, harassment, etc, risk level and potential impact to the organisation or public interest.

High Importance: Immediate Threat to Life and/or Safety; Organisation-Wide Fraud; Involvement of Senior Executives Recommended Action: Immediate Escalation to Board of Directors; Engage Outside Counsel. Moderate Importance: Localised Policy Violation; Mid-Level Management Mismanagement; Repeated Misconduct. Recommended Action: Internally Investigate; Report regularly to Compliance Function. Low Importance: One-Off Incident; Minor Complaints; Question About Company Policy. Recommended Action: HR Resolution; Keep Track of for Trend Analysis. Central to the assessment is the principle of neutral inquiry. Investigators must assess the credibility of a report submitted anonymously based upon the

report's specificity and clarity of information, as well as the availability of corroboration, rather than simply dismissing an anonymous report for lack of a named complainant.

Investigation Phase: It maintains fairness and Impartiality. The entire whistleblower system's credibility relies on the perceived and actual fairness of the investigation. Neutral fact-finding is essential, as investigators must refrain from confirming existing biases, as well as filling in the gaps with assumptions or conjecture from an anonymous report.

Documentation and Audit Trail: Each action must be documented. Actions taken must be documented in a log to provide a complete record of the investigation, i.e., interviews conducted, documents reviewed, and decisions made.

FINANCIAL INCENTIVES AND DILEMMAS (THE GOLDILOCKS PROBLEM)

The Goldilocks phenomenon has elicited continuous discussions among governmental representatives about the level of incentives to provide for whistleblowers. The key aspect of this situation is understanding the range of appropriate incentives: Too small and they would not compensate for the risk and cost incurred by the whistleblower, while those that are too large may attract frivolous allegations or even malicious intent. Many proponents of the bounty model in the United States argue that a successful whistleblower can assist authorities in uncovering crimes that are ‘hidden’ from the majority of society, including things such as price-fixing, tax evasion and foreign bribery. These crimes are rarely captured by an auditor's report because the auditor does not have the same access to information regarding the crime as do those directly involved in it. The high ‘costs of information’ associated with committing crimes are an effective barrier for the vast majority of the population from becoming privy to the ‘conspiracy’ and thus helping to uncover these hidden crimes. The lack of information results in those closest to the crime having access to all necessary documentation to uncover the crime. Finally, the bounty programs in the United States have been incredibly successful, with the government recovering a total of over $46 billion in revenues pursuant to the False Claims Act from 1986 to 2020, with whistleblowers receiving over $7.8 billion. Additionally, the bounty model creates a ‘distrust effect’ among those committing a conspiracy. If the individual who first reports a crime may receive a multi-million-dollar reward while all other individuals who were involved face the possibility of going to jail, the incentive for those involved in the conspiracy to continue it will be substantially reduced.

Building a Speak-Up Culture: The Dangers of Not Speaking Up. As organisations move away from a traditional hierarchical structure to a more open networked environment, there is the emergence of new challenges with how ethical corporate governance will occur and how internal communication will happen. One of those changes is fostering a 'speak-up' culture where all employees across the organisation can report wrongdoing, illegal activity, provide feedback, raise concerns and share suggestions without fear of retaliation. Creating this culture is not just a component of a compliance Program; it is an integral part of the organisation's integrity and its ability to be sustainable into the future. When employees can voice their opinions safely and have them responded to, the organisation is able to establish a strong early warning system to inform management of potential issues, risks or violations before they become large-scale.

Effect: Out of the many risks that have been stated about an organisational culture of 'silence,' the lack of a 'speak-up culture' stands out as one of the most significant and overlooked. Silence is the ultimate destruction and can turn what appears to be a simple lapse in ethical conduct into a major scandal that has significant implications for shareholder value, brand reputation, and the possibility of a catastrophic regulatory action. Historically, there have been numerous instances of corporate failings that have demonstrated a repetitive pattern of behaviour and could have been avoided if there had been a means for the workforce to communicate the issue related to the failing, but rather had faced cultural barriers in doing so that prevented them from voicing their concerns. As a result, the modern-day leader must understand the components of a 'speak-up culture,' as well as the avenues of protection afforded to whistleblowers. The essence of a 'speak-up culture' is one where employees have the ability to openly share their opinions, and it is accepted. A 'speak-up culture' also rewards employees for questioning the status quo and providing opinions that are contrary to the majority of the organisation. This change of environment will shift the burden of ethical behaviour from the compliance function to the entire organisation. When comparing compliance hotlines with creating a culture where individuals feel comfortable voicing their opinions regarding potential policy violations should occur before they occur they differ significantly. When using a compliance hotline, violations are reported after they occur; however, when speaking up (i.e., creating a 'speak-up culture'), individuals have additional opportunities for voicing a minority view that was previously unavailable, from which there is more possibility of receiving differing opinions than would normally be received through traditional communication. In addition, where employee behaviours are identified to create unsafe environments or non-compliant behaviours, organisations may develop methods for

correcting the faulty behaviours prior to being sued due to not taking appropriate steps. Additionally, organisations that have an established speak-up culture often attract more purchasers, clients and higher calibre applicants who wish to be associated with a company that is globally recognised as having high-level ethical standards.

Psychological safety is the main underpinning of disclosure. Professor Amy Edmondson of Harvard Business School popularised the term psychological safety to represent a shared belief amongst employees within an organisation that the workplace is free from detrimental impact associated with risk-taking behaviour. Therefore, employees believe that they will not experience negative consequences for speaking up about their beliefs, such as opinions, questions, concerns or errors. Whistleblowers will likely not use whistleblower protection mechanisms (e.g., hotlines, policies) if the required base foundation of open communication, dialogue and trust does not already exist.[10] These anti-retaliation measures cannot be effective unless employee feedback, assessment, or acknowledgement is obtained and maintained on an ongoing basis, and an open and trusting environment is created to obtain and assess input from employees. By recognising employees' contributions, leaders create an atmosphere for employees to feel valued and provide an additional mechanism for developing trust. Leaders should also be transparent about their own errors or failures to create a sense of security with their ability to take feedback or input from employees. When a leader has made an error, they must publicly acknowledge the person or people who identified the error, the corrective action taken and what has changed as a result to promote fairness in their relationship with employees. This will develop trust between the leader and the employee and develop the open and secure environment necessary to establish a trust-based culture. One of the most important components to building trust is credibility; without credibility, there is a risk that trust between the leader and employee will not exist. If you would like to work on developing your qualifications as a leader with experience behind you, please do not hesitate to contact me to discuss this with me. Leaders must demonstrate their commitment and loyalty towards their organisation both through their verbal communication and through their actions/behaviour towards employees. To do this, ethical measures of performance should be included in evaluating executives' performance, and examples of leaders

[10] Amy Edmondson, 'Psychological Safety and Learning Behavior in Work Teams' (1999) 44(2) Administrative Science Quarterly <https://web.mit.edu/curhan/www/docs/Articles/15341_Readings/Group_Performance/Edmondson%20Psychological%20safety.pdf> accessed 02 May 2026

acting on ethical issues should be collected so they can be used when demonstrating evidence of the leaders having acted on an employee's concern when determining their credibility. Ultimately, if an employee believes that his or her employer will do the right thing when a concern is raised, the likelihood that he or she will report their concern increases significantly. Maintaining a high 'say/do ratio' will increase the likelihood of creating an environment where employees feel safe to speak up.

Theoretical Perspectives on The Reasons Employees Do Not Speak Up and When They Do Speak Up. To understand the reasons why some employees will speak and why some will not speak, it is helpful to understand the underlying social and ethical processes. Two of the main theoretical frameworks that can be utilised to understand the reasons employees may choose either to report or not report are Moral Judgment Theory and Power-Dependence Theory.

Moral Judgment Theory states that many people will report wrongdoing when there is a high level of moral concern, regardless of the benefit to them. Reports of wrongdoing often go against the self-interest of the person making the report because of the emotional and psychological impact of reporting and the low probability of a benefit being derived by the reporter. Moral Judgment Theory states that moral judgment will be a combination of rational factors: knowledge of moral codes and application of logic to determine violation, and non-rational factors; emotional, intuitive type responses.

Power-Dependence Theory: Power-Dependence Theory views whistleblowing as an influence process in which the whistleblower seeks to gain power over others or the organisation by persuading the 'dominant coalition' to act against a specific wrongdoing to contravene a given wrongdoing. The organisation's response, remediation, inaction, or retaliation, is an exertion of power intended to maintain or restore the preferred balance of power. Whistleblowers remain particularly vulnerable in organisations where protective policies clash with internal power structures or market pressures. When retaliation occurs, it is often a defensive move by the dominant coalition to suppress a perceived threat to its authority.

Impact of Business: The presence of a sustainable culture within an organisation and its associated financial return on investment is a major factor in creating an environment where employees feel comfortable speaking out. In addition to providing the business with an opportunity to reduce its financial impact, they allow for the long-term survival and financial

success of that organisation. A strong link has been noted between effective business risk management, sustainable practices and performance. A company's ability to create value for its shareholders is enhanced when they consider risk in the development of its sustainable strategy, as these companies are also more resilient. The return on investment associated with having a culture that supports employee speaking up does not solely relate to external fines imposed; it also includes daily operational savings achieved through reducing the costs associated with doing nothing. While employees would not typically think of all the 'doing nothing' costs incurred in entering data manually, for example, through employees leaving the organisation or through an inability or unwillingness of the organisation to solve conflicts, there are significant savings associated with those costs. Ethisphere states that 'World's Most Ethical Companies' have statistically outperformed their non-ethical competitors by an average of 8.2 percentage points or have accomplished this by utilising the 'Ethics Premium.'[11]

Reporting on Environmental, Social, and Governance (ESG) includes creating a culture that encourages employees to speak up internally and improve internal corporate governance, which is essential for proper governance according to ESG standards. Sustainability Reporting will reduce corporate exposure to reputation or economic losses as a result of regulatory fines or disruptions in the supply chain, among other types of risk. There is an ongoing disconnect between Enterprise Risk Management (ERM) processes and Sustainability Reporting; of the actual material sustainability risks reported, generally only 29 per cent are also reported in formal ERM filings. A company that has a culture promoting speaking up will be able to close the gap between ERM and Sustainability Reporting because, as sustainability-related risks continue to grow (ex, human trafficking, environmental issues, cyber vulnerabilities), they will be identified and held accountable before the corporate world knows about them through a public scandal.

Future Trends: There will be a new type of risk and opportunity for businesses at the cross-section of Artificial Intelligence and whistleblowers, which will also create a new group of AI whistleblowers in 2026 due to the fast development of AI. These individuals will report on unfairly using or manipulating an AI algorithm or using 'agentic' AI improperly; they will have

[11] Anne Walker, 'Ethisphere Announces the 2024 World's Most Ethical Companies' *(Ethisphere,* 04 March 2024) <https://ethisphere.com/news/ethisphere-announces-the-2024-worlds-most-ethical-companies/> accessed 02 May 2026

information to share about unfairly using or manipulating an algorithm. AI Detection: Researchers working independently and regulators purchasing access to AI will utilise AI to help them analyse vast quantities of data from both public and commercial sources for the detection of fraud on a scale that has not previously been possible through manual methods. This will create a movement away from a government-centric enforcement model and toward a distributed enforcement model where…

Eliminating Fear of Retribution: Promoting and sustaining a 'Speak Up!' culture requires a long-term commitment from all levels of the organisation. In order to eliminate fears of retaliation and to end the silence, organisations must focus on these three pillars: leadership accountability, psychological safety, and a solid internal reporting mechanism.

Leadership Responsibility: Leaders are responsible for how they respond to issues reported to them and how they implement whistleblower protections. Additionally, performance evaluations completed for all managers will contain metrics about anti-retaliation behaviour.

Employees and managers must receive regular ongoing training that includes a strong definition of retaliation, where to report concerns related to retaliation both internally and externally, and skills to assist with resolving conflicts. Additionally, this training includes local retaliation laws and is provided in the appropriate language. Leaders should continually assess the feedback they receive from reporting patterns, including the number of total reports made, the number of case closures, and the verification rate. A healthy report will help leaders recognise those trends and what caused them. For example, if there is a sudden increase in the number of reports, this may indicate an increase in trust or other maturity of the ethics program, rather than an actual increase in employee misconduct.

THE DANGERS OF SILENCE

The Case Studies of Corporate Failure demonstrate the extreme negative effects of a culture of silence. Most of these disastrous events (like the scandals at Enron and Boeing) fuse a general pattern for employees/customers; the corporation failed to respond appropriately to employee/customer feedback because the corporation's leadership was focused on short-term profit rather than abiding by a business's established long-term values. Enron Corporation's many toxic traits led to its ultimate demise. Using fraudulent financial practices (i.e., false

accounting methods) to await the appearance of profit & hide losses caused severe problems for both the business and its employees.

The 'rank-and-yank' style of performance appraisals used at Enron also created a very high level of intimidation & an environment in which an employee who challenged management regarding any business decision was primarily viewed as disloyal. Due to this strong motivation to appear altruistic to management, employees felt that to get ahead and legitimise their own success at Enron, most employees had to do it illegally ('Go along to get ahead'). In addition, whistleblowers were systematically removed from the work environment, and the Board members were generally unwilling & unable to pose difficult questions concerning the multitude of complex financial products created by Enron that only they could not understand. Over the entire life of Enron Corporation, Enron lost $74 billion in market capitalisation, along with 20,000 jobs; thus demonstrating the effect of a culture of silence.

Wells Fargo employees were involved in creating millions of unauthorised accounts in the name of reaching aggressive sales goals, reflecting that the cultural aspects of Wells Fargo created an environment that was structured to support and reward employees for engaging in illegal acts as a result of unrealistic incentive programs. Those employees who reported the illegal conduct occurring at the company were subsequently terminated for retaliation against their whistleblower actions by either the CEO or human resources. This case study demonstrates how placing a higher value on trust as opposed to achieving sales results leads to severe reputational damage to Wells Fargo, as well as billions of dollars in regulatory fines.

The 'Dieselgate' scandal at Volkswagen, in which engineers felt there was no way to speak up for fear of being reprimanded by their superiors, created enormous pressure on engineers to use available resources and meet targets. As a result of this environment that discouraged speaking up, engineers devised software so that VW could cheat on emissions tests. Similarly, Boeing had numerous employees internally reporting design issues with the 737 MAX, all of which were ignored by management in pursuit of profit. In both situations, the creation of a culture that permitted technical and ethical failures to rise to the level of deaths and/or financial ruin occurred as a result of a lack of a speak-up culture.

CONCLUSION

Whistleblowing has become an integral part of the corporate structure. The traditional corporate governance model has changed from a strictly top-down hierarchy to a more decentralised and watchful model. In the past, whistleblowers were viewed as individuals who spoke out against their employer, making them look like a traitor or a disloyal employee. In today's global environment, whistleblowers are now seen as a necessary part of preventing fraud, reducing risk, and building long-term sustainability of operations. This is supported by the fact that many countries have some form of corporate culture or legal protection for whistleblowers, while the United States operates under an incentivised and bounty-based system for whistleblowers, and many European countries operate under something similar but have a more structured approach with multiple tiers of reporting. Furthermore, India and other developing economies are also establishing laws to protect whistleblowers. As the demand for transparency continues to become not only a legal requirement but also a cultural expectation, simply having a whistleblower policy is no longer enough; with the recent string of corporate failures, we have seen that an organisation can lose billions of dollars in market capitalisation and damage to its reputation simply by maintaining silence about what is going on inside of it.

Present-day leadership needs to champion psychological safety as the bedrock of real cultural integration in terms of disclosures. Therefore, by applying globally accepted best practices such as the ISO 37002 standard[12] with sophisticated digital platforms, leaders can eliminate barriers to entry for whistleblowing incidents. Organisations that engage independent and objective providers will give workers a safe, neutral environment for raising concerns before they escalate to formal disputes. As a result, by generating an authentic speak-up culture, organisations will deliver quantifiable benefits, referred to as an Ethics Premium, which, in turn, allows them to consistently outperform their competition. Because of the increasing complexity of ESG reporting and the uncertainties associated with the growth and deployment of AI, organisations now face levels of corporate risk like they never have before. Ethical behaviour is no longer just the responsibility of a compliance function; therefore, organisations that act within the three pillars of accountability for leaders, psychological safety for employees, and established internal systems for employees to report problems will create an environment that alleviates the fear of

[12] *Whistleblowing management systems — Guidelines* (International Organization for Standardization, 2021)

retaliation, thus changing whistle-blowing from a reactive mechanism to a proactive strategy for ongoing viability and growth.