2025/05/05

The Last Knight: Protecting the Whistleblower, When Disclosure Becomes Fatal

Whistleblowing is not a grudging compliance exercise with the Protected Disclosures Act 26 of 2000 (PDA) and Protected Disclosures Amendment Act 5 of 2017 (PDAA). Instead, it should be reframed as a critical early warning system that protects employees, the organisation's reputation, financial health, and ethical culture.

In a functional corporate environment, the employer's best practice approach hinges on one core principle: making it psychologically safe and procedurally simple for an employee to raise a concern. An employee who trusts their internal system has no reason to go externally to the media, regulators, or social media, which invariably leads to reputational damage, even if the disclosure is ultimately found to be unsubstantiated.

1. Understanding the Legal Framework

The Protected Disclosures Bill, 2026 (currently open for public comment until 14 May 2026) intends to develop the existing whistleblower protections. Some major changes: expanding key definitions (good faith, disclosers, employee and related persons), timelines and accountability for investigations, criminalising the exposure of whistleblowers' identity and acts of occupational detriment, complaints and enforcement mechanism, and financial incentives for certain categories of whistleblowers.

Legal concepts to master and exceed:

- **Good Faith is Expanded:** A disclosure is considered to be made in good faith, even if there is an ulterior motive. An employee only needs a reasonable belief that the information shows wrongdoing. This implies that an employer cannot attack a whistleblower's motive; they can only challenge the reasonableness of their belief.

A whistleblowing policy must reflect this, focusing on the substance of the report, not the perceived attitude of the reporter.

- **Scope of a Protected Disclosure:** The PDA covers a wide range of impropriety, from criminal offences and legal non-compliance to miscarriage of justice, health and safety dangers, and environmental damage. Best practice extends this definition internally to include any serious breach of the company's code of conduct; this demonstrates a commitment to a higher ethical standard.
- **Occupational Detriment:** The PDA defines occupational detriment broadly (dismissal, suspension, demotion, harassment, intimidation, transfer against will, etc.) and provides remedies, including compensation and 'automatically unfair' dismissal protection under the Labour Relations Act. Best practice means not just prohibiting and preventing these acts but actively guarding against subtle, systemic detriments like social ostracism, exclusion from key projects, or unfair performance reviews.

In the current South African environment, a best practice model requires a profoundly serious and necessary shift in perspective. The existing reality demands a context where whistleblowing can be a death sentence, a grim truth in South Africa. The assassination of whistleblowers or the credible threat of it, fundamentally reclassifies an employer's duty from "best practice" to a human rights obligation and existential duty of care.

The killing of individuals who expose corruption linked to organised crime and state capture networks that have infiltrated the state and private companies is not an abstract risk. For an employer, the knowledge that their workplace might harbour conduct for which people kill, means the standard corporate whistleblowing manual must be amplified. The entire framework must be rebuilt on a primary premise: You are not just managing a report of misconduct; you are managing a life-threatening security crisis**.**

2. Reframing Protection: From Procedural Fairness to Physical Security and Anonymity

In a context where fraud and corruption are rife and lethal, the primary tool of protection is not a policy against victimisation; it is an impregnable wall of absolute anonymity and physical security.

a) Necessity of Absolute Anonymity, Third Party Channel

An internal reporting line to a manager or HR head is no longer a safe first step; it is a potential tripwire. The information chain is too short, and the risk of the report leaking back to dangerous actors is catastrophic. This extreme context demands:

- **External, Independent, Forensic-Level Hotlines:** Anonymity must be technologically guaranteed. The service must not have caller ID, must not record voices, and must use a blind, two-way communication portal where the whistleblower uses an alias and a unique, system generated password to check for

messages. Data must be encrypted and stored offsite, outside the reach of local compromised networks.

- **Technology Free Dead Drops:** Any digital trail can be a vulnerability. The policy must provide a physical, untraceable method. This could be a secure, anonymous postal lockbox that goes directly to an external forensic company, or a pre-agreed, physical "dead drop" managed by the forensic company. The message to the employee is: "You can tell us without your phone, your computer, or your identity ever being in the system."

b) <u>Activate a Crisis Security Protocol, Not an HR Procedure</u>

The moment a disclosure is received that implicates serious organised crime, physical threats, or involves sums that make killing a rational business cost for the perpetrators, an HR-led process must immediately be subordinate to a crisis security protocol. This protocol is a prewritten, rehearsed plan that kicks in automatically based on a threat classification matrix.

The protocol's immediate steps are:

i. **Secure the Whistleblower's Identity:** Give the casefile a codename. The whistleblower's actual name, if known, is siloed on a strictly need to know basis e.g. the two-person rule: one forensic lead, one senior independent legal counsel. Not even the Group CEO automatically needs to know the name.

ii. **Immediate Physical Security Assessment & Facilitation:** If the whistleblower's identity is known to the company (e.g. they reported in person), the employer's non-negotiable duty is to fund and facilitate a professional physical security assessment. This is not the same as a wellness check. It is a trained, vetted security professional assessing their home security, travel routes, digital footprint, and vulnerabilities. The employer must offer and fund immediate protective measures: relocation to temporary secure accommodation, travel changes, and proactive security presence if the threat assessment warrants it. This is the minimum cost of receiving such a disclosure.

iii. **A Pre-Established Disappearance and Resignation Fund:** A harsh reality: the safest outcome for a whistleblower whose identity is known internally may be to leave the company entirely. The investigation and any subsequent state witness protection are long, slow processes. The employer must have a dedicated, independently administered fund to provide an immediate financial bridge (a lifeboat grant) that allows the employee to resign and relocate without notice and without financial ruin, as a direct protective measure.

3. Reframing Education: From Ethical Culture to Web of Safety

The education strategy flips from "speaking up is safe" to a careful, sober, and highly strategic code of "silence for good". The goal is not broad cultural cheerleading; it is equipping a small number of people with the tools to survive a life-threatening circumstance.

a) "Keep Yourself Safe First" Mandate

Standard ethics training says, "If you see something, say something". The new risk aware mandate must be: "Your life is worth more than a report. Do not become a martyr. Your first duty is to get out safely, and our first duty is to give you a way to do that". This is a shift in messaging that builds faith in the company and its process.

b) "Know the Threat" Education for High-Risk Groups

This is not for all employees. General, graphic discussions can cause panic. Instead, it is a mandatory, confidential briefing for those in high-risk gatekeeper roles e.g. finance, procurement, supply chain, internal audit, and senior executive assistants. The content, delivered by external specialists including a forensic investigator and a trauma counsellor, should cover:

- The red flags that a scheme is not just internal fraud, it is syndicated (e.g. unexplained affluence of a colleague, presence of unknown external consultants giving orders, physical intimidation as a management style).
- The absolute rule: If you have such a suspicion, do not document it on work systems, do not search for evidence, and do not discuss it with colleagues or your manager**.** Engage the anonymous channel to simply state, "Look in X area to uncover Y".
- A comprehensive briefing on how organised crime infiltrates companies. It demystifies the threat, framing it as a predatory business model, not just individual bad behaviour or a misstep.

c) Training a "Special Forces" Team

The company cannot rely on its standard HR team to handle a disclosure that carries a mortal threat. It must identify and train a small, vetted, ring fenced crisis management cell (the special forces for this situation). This cannot be a standing committee whose membership is publicised; it is a dormant capability, activated by an anonymous call to a designated external forensic auditor or legal counsel. This cell's training should include:

- **Operational Security:** How to communicate using encrypted channels, how to handle physical evidence without contaminating it or leaving a trace, how to commission a covert investigation that cannot be traced back to a human source.

- **Trauma Focused Strategy:** Recognising that the person on the other end of an anonymous chat is likely in a state of abject terror. Every word, every delay is a potentially fatal signal. Training is on how to communicate with the source using pre-determined code words for escalating danger.
- **State Engagement Protocol:** Knowing exactly when and how to safely engage, e.g. the Directorate for Priority Crime Investigation (Hawks) or the National Prosecuting Authority without exposing the source. This involves external legal counsel acting as a professional buffer, handing over information in a way that protects the whistleblower's identity under legal privilege until a plan for their safety is formalised by the company or state.

The fundamental fact is that the employer must view themselves, in this moment, as a safe house in a warzone. The employer's actions, policies, and duty of care are no longer just civil obligations. A failure to create an absolutely secure channel or to proactively fund a lifesaving security intervention for a whistleblower is a betrayal that reaches the level of potential civil and criminal liability for gross negligence.

4, The investigation

The entire investigation methodology must be reverse engineered to prevent the situation where the process of justice inadvertently becomes the instrument of exposure and ultimately an injustice.

This requires a radical departure from standard corporate investigative procedure, from a fact finding model to an intelligence gathering model, where the protection of the source is a higher priority than the immediate building of a disciplinary or criminal case.

a) The Foundational Principle: Decoupling the Source from the Evidence

The disclosure is treated as a single use key that unlocks the investigation, but it is never used as a building block for the evidence. The information provided by the whistleblower is classified as human intelligence, not evidence. The entire goal of the investigation is to find the exact same information from an independent, non-human source or to structure a probe so broadly that it appears the discovery was inevitable and not triggered by a tip-off.

b) Legal Privilege as a Shield: The Role of External Counsel

The single greatest structural protection against exposure is to irrevocably intertwine the investigation with legal professional privilege. The investigation is not structured as a management or HR probe. It is a privileged, confidential fact-finding exercise to allow the company to obtain external legal advice about its own legal exposure.

- **The Mandate:** External counsel (with an independent duty of confidentiality) formally commission the forensic investigators.

- **The Privilege Wall:** All investigative reports are addressed to the external counsel and marked. In any subsequent litigation or disciplinary hearing, a strong argument exists that the underlying report and its workings are protected from disclosure. It becomes significantly harder for an accused party to demand the source and origin of the investigation.
- **The Buffer:** The external counsel acts as a physical and legal barrier. They receive the whistleblower intelligence. They instruct the investigators without revealing the source, translating the intelligence into broad, independent, and justifiable investigative steps. The client instructing the investigator is a lawyer, not the HR director or management.

c) Controlled Revelations: The Alternative Source

Sometimes, the theory of parallel source construction must be extended into active, highly controlled disinformation to protect a source whose identity is on the verge of exposure.

- **The Anonymous External Tip-Off:** If a specific document must be requested and the request will inevitably draw attention, the investigative team might deliberately handle it in a way that suggests an external complaint.
- **The Red Herring Interview Line:** In an interview, an investigator can deliberately use a vague, broad, and inaccurate source reference; e.g. suggesting a computerised, system generated flag. This shifts the imagined source from a human being to a machine, or to a vague, faceless process. The goal is to contaminate the perpetrator's mental model of where the threat came from. They are left chasing ghosts.

d) The Unavoidable Exposure Protocol: Preparing for the Worst

There are scenarios where the whistleblower's identity as a witness, not just a source, is unavoidably exposed. This usually happens when the case must go to a criminal trial, and the whistleblower is the only person who can testify to a crucial element of the crime, like a verbal order. The protection strategy then shifts from preventing exposure to ensuring survival through and after exposure. This is the activation of the resourced, and rehearsed Crisis Security Protocol.

The revelation of the whistleblower's identity is often the definition of an investigative failure. It is the result of a choice to prioritise the speed and convenience of building a case over the methodical, more expensive, and slower work of parallel source construction.

Your Whistleblower Policy

Don't have a 20 page PDF buried in the HR portal. Build a dynamic, fit for purpose policy. The best practice, in a country where whistleblowers are executed for uncovering workplace corruption, is a definite preparedness to act not just as a company but as a protector of lives.

By integrating robust, human centered protection protocols with a leadership driven education campaign, your company transforms the Protected Disclosures Act from a compliance document into a living contract of mutual trust and ethical resilience.

Partner with Cyclopedic Consulting.

By **Adv. Sannah Pooe** 2026/05/05