BACKLASH

MOST ORGANISATIONS WILL SAY THEY DON'T RETALIATE AGAINST WHISTLE-BLOWERS. THE REALITY IS A LOT HARSHER, SAYS KEITH READ

Whistle-blowing, and whistle-blowers, are rarely out of the news; a whole industry has sprung up around whistle-blowing and it takes just moments to find a myriad of articles and learned papers about the subject. However, there are some practical whistle-blowing realities that organisations need to be aware of – and, crucially, they need to ask themselves whether that 'anti-retaliation' policy, however well-structured and carefully written, really prevents retaliation.

Most companies and organisations now have a whistle-blowing facility, provided either internally or externally, or through a combination of both. Organisations will often first establish an internal whistle-blower facility and subsequently migrate to an external hotline provider, which brings with it a potentially wider range of intake channels – including telephone, email, letter, fax, web forms and manager conversation capture – together with multi-language capability and managed anonymous reporting.

However, organisations often set up their whistle-blower hotline and, with that box ticked, leave it at that. Crucially, they often fail, for example, to make even the most rudimentary test calls to their own hotline. From personal experience, seven test report calls made to an organisation's internally provided hotline exposed an informal triaging process, which resulted in only two of those reports making it all the way through the process. Moreover, the handling of one call, made in a major European language, was so dire and slow that only the most determined caller would have persisted.

IKON

Organisations often underestimate the importance of their hotline infrastructure. So, for example, free-to-call is pivotal when it comes to encouraging reporters to make their call. But achieving that objective in all countries of operation can often appear to be an impossible challenge. The resulting mixed approaches will lead to companies issuing instruction handbooks that run to 30 pages of numbers and complex instructions. The procedures tend to be especially complicated for callers who want to remain anonymous. Clearly, again, this inevitably serves to directly deter callers.

Companies often fail to consider the situation in countries where they have a low employee population, but a high risk-operating environment, with the result that whistle-blowing report volumes often tend to be low, because employees

wanting to make a report are fearful of identification by a simple process of elimination. Put simply, if there are 10 employees and their manager in a country office, then it is not going to be that difficult to identify who might have made a report. There are techniques that can be used to deal with types of exposure issue, but organisations often fail to consider them and, as a result, forego what can often be vital information.

Anti-retaliation policies

The vast majority of organisations have an anti-retaliation or no-retaliation policy for whistle-blowers and, without question, it is clearly the right thing to do. However, most policies are just that – they sit on the shelf and often have little impact on what happens in reality day to day. Indeed, particularly in the case of anti-retaliation, policy communication is relatively poor – often because of a misplaced perception that "retaliation wouldn't really happen here".

Moreover, despite all these no-retaliation policies, it takes just moments to find appalling cases of retaliation – involving some very high-profile and household name organisations – that have taken place on both sides of the Atlantic, and elsewhere.

Organisations invariably find it a challenge to implement effective key performance indicators for their compliance programme, and the question of how to measure outcomes becomes even more challenging when it is related to retaliation.

Professionally, I have seen many instances of retaliation in action. The problem is that it can take many forms; it can take place at organisational, manager and colleague level, and involve both 'hard' and 'soft' retaliation – ranging from hard cases: discipline, dismissal and harassment, right through to soft cases: loss of a whistle-blower's career, including advancement, loss of overtime and other opportunities. Whatever form the retaliation takes, it certainly affects the individual and means that other people will inevitably think twice about whistle-blowing.

Retaliation data

In one case, where I suspected that, in spite of the existence of an anti-retaliation policy, retaliation was alive and well within one particular organisation. I decided to try to look at the whistle-blower data – who the whistle-blowers were and where that information was available – and then link those individuals to data that could indicate retaliation. This data included the individuals' subsequent annual performance review markings, pay rises, bonuses, disciplinary actions and an evaluation of their career progression compared to their peers. Not a full or exhaustive set of data, but a subset that I could work with to get an indication of whether my concerns were real or imagined.

The vast majority of organisations have an anti-retaliation or no-retaliation policy for whistle-blowers

It became obvious within minutes that retaliation was clearly taking place; not everywhere, and not affecting every whistle-blower, but it was there. Moreover, some divisions, departments and locations had a noticeably greater propensity for retaliation than others and, I suspected, some of that was linked to certain managers and senior managers. Confirming that issue was largely beyond manual analysis, given frequent organisational changes and movement of individuals within the organisation.

Some individuals had clearly been high performers prior to blowing the whistle; after that event – at least if the performance review markings were to be believed – their performance had declined sharply and, in some cases, had never recovered; a loss to them, and a loss to the organisation.

The reality

Armed with this analysis, I was at least in a position to raise the issue – the reality of retaliation – and to get the message out there that retaliation was being monitored, however simply and crudely. I would like to think – and there was some evidence to this effect – that retaliation lessened to a degree once that signal had been sent around the organisation. But, clearly, it can take years for patterns to emerge.

Five years on from that particular example, at almost every compliance event, the question of whistle-blowing comes up and the discussion usually turns quickly to the issue of retaliation and anti-retaliation policies. I invariably ask how compliance officers know that their policy is working. Without exception, people reply that they don't, but that they do have a policy. Talking about how even rudimentary analysis could be put in place often turns out to be a 'light-bulb moment'. People start to discuss what simple analysis they could undertake within their own organisations.

Anti-retaliation systems

Going forward, organisations will be able to bring their compliance-related systems – covering whistle-blower hotlines, case management, policy communications and training – together with their core HR data, such as annual performance review markings, pay rises, bonuses, disciplinary actions, career progression, overtime awards and suchlike. This will transform this simple approach into an effective real-time compliance tool – one that enables organisations to be confident that they genuinely have no retaliation – and that they are in a position to prove it.

Keith Read is an independent compliance consultant