CALL IT IN: THE ADVANTAGE OF OUTSOURCING WHISTLEBLOWER HOTLINES

Keith Read
Director, Europe
Convercent
INTRODUCTION

Implementing an effective whistleblower hotline is a crucial element of an organisation’s corporate governance regime—one often mandated by legislation, regulators and industry best practices. However, in that implementation, organisations of every size and shape invariably face a dilemma: should the hotline reside within the organisation, or provided by a suitable third party?

This short whitepaper identifies some of the issues and considerations that organisations need to take into account in resolving that dilemma, whether they’re implementing a hotline for the first time or reevaluating their existing approach and weighing the costs, benefits and value of migration.
A VIEW FROM THE TRENCHES

I formerly served as the Group Compliance and Ethics Director for a £20 Billion FTSE100-listed company that had 150,000 employees and contractors operating in 176 countries. I implemented the company’s first whistleblower hotline: an internal system that leveraged the company’s existing 24/7/365 security helpdesk. This approach worked reasonably well—at face value, at least—in that it we were able to implement a hotline at marginal cost, “check the box” in the eyes of regulators and field reports of alleged misconduct from employees (which, indeed, we did).

However, I became increasingly uneasy about the performance of our internal hotline. Handling a security report was one thing but dealing with a potentially nervous whistleblower and a potentially complex report was another—even with specialist training. Delving into our hotline Key Performance Indicators (KPIs) validated my suspicions: overall hotline performance was variable and, crucially, we were receiving few (if any) reports from our highest risk locations.

I decided to make seven test reports to our hotline, including one in French. The reports were all designed in a way that they should have come back to me as the compliance director because of the report routing rules and procedures in place at the time. I received just two reports, and French translator’s handling of the call were enough to put all but the most committed caller off.

There was informal “triage” being undertaken at the helpdesk. As a result, we were losing a number of reports, and our ability to build a wider compliance risk picture was being compromised.

This experience, coupled with following market and organisational considerations outlined in the following pages, resulted in the board accepting a recommendation that we move to an outsourced whistleblower hotline. Whenever I now speak about whistleblowing and whistleblower hotlines, I always ask audiences how many have made test reports in their own organisations; the numbers are invariably at, or near, zero.

BUILD...OR BUY?

CONSIDERATIONS
As outlined above, many organisations first implement a hotline internally (“build’) and then—for a range of reasons—may move to an external third-party provider (“buy”). Thereafter, they may move to another provider or, indeed, return to an internal implementation.

These decisions can be driven by a wide range of considerations that include, but not limited to:
- Cost comparisons
- Overall whistleblower hotline performance
- External third-party provider relationship
- Data protection performance, and issues
- Case/report management capability and performance
- Translation practice and performance
• Telephony infrastructure costs and configuration/change challenges
• Infrastructure issues (communications, policies, posters, etc.)

INDUSTRY RESEARCH
A number of studies have been undertaken on whistleblowing, some of which address the Build or Buy dilemma by examining whether a whistleblower is more likely to make a report to an internal or external hotline.

These studies often come to directly contradictory conclusions: the internal argument being that whistleblowers will be more confident because they believe their information will be kept in-house, and the external argument being that whistleblowers will be more confident because they believe their information is less likely to be leaked or handled by someone they know.

This point should not be underestimated; whistleblowers invariably consider their information to be very sensitive (regardless of whether it actually is) and this consideration often factors disproportionately into their decision processes. Arguably, leak concerns become significantly more prevalent in smaller organisations, which can also play directly into anonymity decisions.

In my experience, a well-communicated and positioned external whistleblower hotline can obviate the perceived issues of data security and confidentiality. On balance, research also come down on this side of the argument.

ORGANISATIONAL LOCATION
One of the biggest challenges of an internal whistleblower hotline is deciding where it should be physically located, managed and operated—both now and in the future.

Clearly, security, compliance and legal are possibilities you could make arguments for. There are also units where the whistleblower hotline should not be embedded—including, for example, within the finance division.

However, evolution in the organisation’s structure and business can bring with it significant and unexpected challenges in terms of whistleblower hotline management, resourcing and day-to-day prioritisation.

From personal experience, what started as a reasonably-resourced security helpdesk progressively became under-resourced as cost-cutting became a necessity. This had the direct consequence of drastically longer call waiting times, and a greater proportion of incomplete calls. By comparison, an external whistleblower hotline provides a degree of organisational “buffering” against such organisational shifts.

COMPARATIVE COSTS
As part of a wider review of my former company’s cost of compliance, coupled with a compliance return on investment (ROI) analysis, we undertook a comprehensive analysis of the internal whistleblower hotline operating costs.
There is a general perception that using a suitable third party to implement an external hotline is more expensive than using an internal system. This may be the case for a very basic internal hotline—one that uses an answering machine-type functionality, for example. However, developing, implementing and maintaining a full-service, robust and demonstrably compliant whistleblower hotline programme internally is deceptively expensive. The costs of around-the-clock resourcing, training, IT, telephony, technology and translations, amongst others, are often underestimated or not fully considered.

Ultimately, the true whistleblower hotline costs are far more than originally estimated in cost comparisons, while the implementation and operational challenges serve as an ongoing management distraction for those charged with responsibility for the hotline. That distraction often serves to directly diminish effort and focus on utilising the very information that the hotline was set up to gather.

Moreover, an external whistleblower hotline provider can achieve significant economies of scale and, hence, cost—even allowing for a margin of profit—by providing a wider range of services to a larger group of organisations. The volume of reports to an internal whistleblower system may not warrant investment in all reporting channels which then turns into a so-called hotline “Catch-22.” Also, arguably, an external whistleblower hotline provider also brings with it recognized credibility, industry reputation and systems performance, including availability.

As organisations foster the trend towards opening up their whistleblower hotlines to all or selected third parties (including suppliers, contractors, consultants, wholesalers, retailers, agents, resellers and so on)—whether it be for reasons of corporate protection, best practice or mandate—the three-way equation of resourcing, performance and cost can quickly become critical.

KEY CHALLENGES

The continuing development of, and variations in, whistleblower hotline legislation clearly brings with it many ongoing challenges. Amongst several others, these challenges center around issues related to geography, authorised use of the hotline, data privacy, limits on acceptable hotline issues (such as accounting, bribery, etc.) and data transfer. This is another example where an external whistleblower hotline provider can bring to bear extensive experience and expertise gained in a number of implementations on behalf of multiple clients, usually spanning a range of geographies.

Telephony infrastructure can also represent a significant challenge in a whistleblower hotline implementation programme. However, done well, it can be used to reduce both cost and perceived barriers to callers, while retaining the flexibility to migrate the hotline downstream should the need arise. This is an often overlooked aspect of hotline implementation and is an area where a capable external third-party provider can bring significant added value.

A further key challenge clearly relates to that of case management. One of the comparative KPIs that we focused on in preparation for migration to the externally-provided whistleblower hotline was that of case handling performance. We experienced a very significant long-term improvement in this area and concluded that it was largely because of the more consistent, structured and tenacious approach taken by the external provider—and the consequent perception that a whistleblower-hotline related communication had to be dealt in a conscientious and timely manner.
RETALIATION - THE REALITY
What is often overlooked in the Build or Buy debate is the added value, outside the core hotline provision of a whistleblower hotline, that an external provider can bring to the wider compliance performance of an organisation.

For example, the vast majority of organisations have a non-retaliation policy for whistleblowers. No one would argue that 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.

Moreover, despite all these non-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 in companies of all shapes and sizes, around the world.

Organisations invariably find it a challenge to implement effective KPIs for their compliance programme. When it comes to retaliation, measurement becomes even more challenging.

A series of issues and an ad-hoc discussion with a hotline vendor made me attempt to look at the whistleblower data—specifically who the whistleblowers were and where that information was stored. I also linked those individuals to data that could be indicators of retaliation, including their subsequent annual performance review markings, raises, bonuses, disciplinary actions and career progression against their peers. It was not a full or exhaustive set of data, but certainly a subset that I could work with manually to get an indication of whether my concerns were real or imagined.

It wasn’t imagined. It became clear within minutes of sitting down with that data—limited as it was—that retaliation was occurring. It wasn’t happening everywhere, and didn’t affect every whistleblower, but it was there. Some individuals, for example, had clearly been high performers prior to blowing the whistle. After that event—according to performance reviews—their performance declined sharply and, in some cases, never recovered. This is a catastrophic loss to the reporting party as well as to the organisation. Even a rudimentary analysis as this can help build or augment your case for taking your hotline elsewhere.
OVERALL
This short whitepaper considers some of the challenges that organisations face in resolving the whistleblower hotline Build or Buy dilemma, regardless of the point that they are at in their hotline provision lifecycle, by highlighting both the short- and long-term elements of those challenges, and some practical tips and lessons learned from the front lines.

Overall, a trusted and reputable external provider will bring far more than just the whistleblower hotline to the overall compliance performance of an organisation. A carefully selected hotline system will also—crucially—provide a key element of a comprehensive compliance toolset, designed to effectively address the legislative and regulatory challenges that are in place and on their way.

ABOUT THE AUTHOR
Keith Read is an award-winning thought leader and expert in compliance, ethics, culture and governance and current Director of Europe for Convercent.

He was formerly the Group Director of Compliance and Ethics for BT (British Telecom) in London and is a past winner of the Compliance Register’s Best Compliance Officer award, when he also won the Best Compliance Company award. He was subsequently the subject of a full-page Daily Telegraph national press article - ‘Compliance and Science’.

Keith has an innovative and practical approach to compliance, using techniques such as ‘Compliance not Complacency’ - whilst recognizing the ‘Cost of Compliance’. He advocates takes a new and highly original approach to the challenge facing all compliance officers; that of changing the significant ‘push’ needed to deliver and maintain an effective compliance programme into employee ‘pull’. Keith is a frequently-requested international speaker, drawing on his wide-ranging practical experience of compliance, including the Bribery Act and Anti-Bribery and Corruption. His thought-provoking ideas and infectious enthusiasm appeal to diverse compliance, ethics and governance audiences, and readers, worldwide.