Leveraging a crisis: are you looking beyond tech and using the full compliance toolkit?

Katie Vickery, Global Compliance Partner, and Chris Wrigley, Global Compliance Associate Director, at Osborne Clarke LLP consider the practicalities of crisis management, including how best to be prepared, and the importance of capturing lessons learned from major compliance incidents

What was top of the agenda for your business's last Board meeting? Was it a compliance issue?

If your business has been through a major compliance issue in recent times, the answer may well be "yes". The focus might have been on incident response, dealing with a regulator or legal fallout, or possibly consideration of the post-incident response. At this point, your Board is likely to have been focussed on the detail in a way they will not be (given the competing demands on their time) in perhaps, six, twelve or eighteen months.

Once a compliance crisis has been dealt with, the Board, understandably, wants to turn its attention to the next major business challenge or opportunity. Everything else cannot simply be put on hold while compliance is dealt with.

Although it may be difficult to see it as such at the time, the aftermath of a crisis, therefore, presents a rare opportunity to effect real, cultural change in an organisation, and to get buy-in at the most senior level for actions that can put your business on a sounder compliance footing long into the future. This makes commercial (as well as legal) sense, because if you do it well, the occurrence of compliance issues which draw in Board time and resource should be minimised, and the legal and compliance team will have greater capacity to deal with exceptions, having put in place the structure and routines to manage and nurture a day-to-day compliant culture.

Such thinking was the starting point for a series of workshop sessions that we ran across Osborne Clarke's UK offices, in which we brought in-house counsel together to explore the breadth of the compliance tools that businesses have available to them, how such tools are really being used, what good compliance looks like and to share best practice and learning.

In this article, we share some of the insights coming out of those sessions.

Make the follow-up count

Nearly half (45%) of those attending the workshops, who had been through a crisis situation, reported that there had not been a meaningful debrief and review after the crisis was over.

While it can at times be a painful process, failing to carry out a proper post-incident review is not just a missed opportunity, it is a hostage to fortune if the same issues arise again, particularly if they reveal systemic problems.

Regulators are likely to question why, having become aware of a risk once, the business had not dealt with it. A business that has been through an incident may also be higher on the regulator's radar for some time to come. The occurrence of an incident, therefore, alters the risk profile for the business and should reduce the tolerance for any non-compliance in the business.

The final output from an internal investigation can vary considerably. While the primary purpose of an investigation report is to focus on the incident, often it should go beyond identifying the causes of the incident, and should contain concrete recommendations for improvement; with responsibilities and timings associated with each action. Where there is a concern about identifying improvements in the middle of an incident, recommendations can still be made during the post-incident briefing.

The investigation report is a key touch point with the Board. Getting Board buy-in for the action list, and building in a mechanism for reviewing progress at set intervals, will help to focus minds in the months to come. It also means that there is an opportunity to ensure the recommendations cover not just the short-term fixes connected to the identified behaviour, but also take account of what appropriate actions should be taken to prevent such issues arising in future.

This second element, if it is to be effective rather than an headache for those implementing it, should take into account the business' wider

approach and aspirations, for compliance. This alignment is important to enable those responsible for compliance to leverage the crisis to improve the business approach going forwards.

This alignment is key to overcoming the challenge of ensuring that recommendations are implemented. The difficulty of following through on recommendations was flagged as a significant issue at our in-house counsel sessions: more than half of those in attendance said that they had received an external report with compliance recommendations that had not then been implemented.

For the most serious incidents, one of the solutions we discussed with in-house counsel , was finding a way of feeding recommendations through the audit committee. A frequent observation was that whilst it can be a challenge to ensure that recommendations from legal and compliance are followed through, those that come through the audit committee are often more strictly complied with. In view of this, the aftermath of an incident could be a good time to establish and formalise the links between the compliance function and the audit committee.

Keep the memory alive

Major incidents are always stressful and, particularly where they have involved harm to individuals, can be traumatic for all involved and not easily forgotten. But people move on to other organisations, and take with them the corporate memory and the experience that comes with it. Post-incident reports and follow-up reviews are useful for ensuring that learnings are captured, but how do you ensure that those learnings are not forgotten?

This is where the power of a crisis can be harnessed by invoking its memory. Incorporating the incident and its learnings into training and case studies that can be rolled out or repeated, can help you focus training towards the specific circumstances and risks faced by people in your business, and help keep the issues at the forefront of people's minds.

You might even want to ask one of those personally involved in an incident to talk to groups in the future about their experiences (or perhaps record a video recounting the impact of the crisis on their day to day lives, including the stress they came under and the impact on other aspects of their lives and work). As effective politicians know, people are more readily influenced by a powerful real-life experience than the abstract concept of risk.

> ***"technology is not a panacea for all compliance ills, and if businesses are not careful it can be an expensive part of the problem rather than the solution. Tech tools, correctly calibrated, can far surpass humans at processing large datasets and spotting well-hidden patterns, leaving humans to do the more qualitatively complex tasks of investigating red flags and determining whether there has indeed been illicit behaviour"***

To tech or not to tech?

Compliance often requires individuals to take actions that are logical and necessary from a risk avoidance perspective. But it can be difficult to get employees to actively do something for the purpose of compliance, rather than to further a commercial or personal goal. 'Nudge theory' is based upon a recognition that human beings often act imperfectly and impulsively.

Small changes to the 'decision environment' can make it easier to 'do the right thing' and can have a disproportionately large effect on behaviours. One way of changing the decision environment is through the use of technology.

Compliance technology typically falls into two categories: the reactive technology that helps you monitor and oversee compliance, and the proactive technology which manages business workflows, and into which compliance processes and 'gates' can be weaved. It is this proactive technology that can help change the decision environment. One striking example that came out of our workshop sessions was linking the payment of expenses to the filing of a report for anti-bribery purposes.

But technology is not a panacea for all compliance ills, and if businesses are not careful it can be an expensive part of the problem rather than the solution. Tech tools, correctly calibrated, can far surpass humans at processing large datasets and spotting well-hidden patterns, leaving humans to do the more qualitatively complex tasks of investigating red flags and determining whether there has indeed been illicit behaviour. It is rarely a case of the tech replacing humans; rather, the tech augments what humans would be able to do on their own.

Nevertheless, there is a risk of tech for tech's sake. So choosing the right tech for your business is critical. To do this you need to be clear about what you want from the tech, and what you do not need. An expensive, all encompassing 'bells & whistles' tech solution, which does not fit with your business, and potentially makes it harder to see problematic behaviour, could be an expensive white elephant and an opportunity lost.

Equally, the 'tech' you need may

(Continued on page 4)

(Continued from page 3)

already be at your fingertips, if you have existing systems which could be harnessed to drive a more compliant culture. For example, one delegate explained that they had removed the feature within Outlook that predicts the email address of the person in the "To:" box. This had greatly reduced the number of emails sent to the wrong address and data being shared with the wrong person.

Tech can provide the tools, but if the tool is not properly used and understood, it can provide a false sense of security. A system that comes to be seen as a tick-box exercise to pass an audit, rather than a tool that requires engagement to reduce risk to the business, can do more harm than good to the compliance cause.

With a dizzying array of tech being touted, when considering any potential new tool, it is helpful to keep in mind three essential questions:

- Is the driver for this a problem that has been identified in need of a solution, or is this a clever solution looking for a problem?
- Is this the simplest way of solving that problem? (Invariably, the simpler solution will be the better one).
- Can the same thing be achieved by using/re-purposing tech that is already in the business?

It is more than a little ironic that a DIY approach to problem solving using existing tools is one of the hallmarks of tech firms. Taking a leaf out of their book can do more to engender a culture of innovation than an over-reliance on new, off-the-shelf solutions. Practically, too, sometimes it may be easier to get people to use technology they are familiar with, than introducing another IT system.

There may even be times when the best approach is to strip away technology. E-learning has come a long way and has much to offer, but might it be more effective for certain purposes to do what one attendee at our sessions did and replace hours of e-learning with a face-to-face session with a member of the legal team? This approach also has the benefit of raising the visibility of the legal/compliance team and establishing or reinforcing personal connections.

It all starts with culture

You can tell the safety compliance culture of an organisation you are visiting relatively quickly. Car parks are well maintained with clear pedestrian walkways. On the stairwells, all employees hold onto the handrails. Fail to do so and you are likely to be called out pretty quickly – regardless of your seniority or of the person calling you out.

If you work in a high-risk industry, like the nuclear sector, chances are you will recognise these signs. In an industry where safety is paramount and businesses are highly-regulated, the safety culture permeates from the shop floor to the very top.

> ***"an effective compliance culture needs to be driven from the most senior levels of a business. This need is why a crisis is also a golden opportunity to make lasting, positive changes. Convince the Board and senior managers why they need to change and you will have a powerful advocate and driver of cultural change"***

Indeed, we all take our cues from above and an effective compliance culture needs to be driven from the most senior levels of a business. This is why a crisis is also a golden opportunity to make lasting, positive changes. Convince the Board and senior managers why they need to change and you will have a powerful advocate and driver of cultural change.

But don't stop there. Track the process through as messages are cascaded down. If there is resistance, influencers in more senior positions can help to reinforce the importance of the message.

At each stage, where you are seeking to get an individual on board, it can help to understand what their motivations are. Broadly, individuals fall into three categories, depending on their motivations:

- *Success* - For some, the overriding motivation is to succeed or win. Compliance targets that are goal-oriented are most likely to be effective with this group.
- *Failure* - Other individuals are motivated by the desire to avoid negative outcomes. Warnings about the sanctions of non-compliance and illustrations of what can go wrong tend to be effective with this group.
- *Ethics* - Compliance is ultimately about doing the right thing. For this group, it can be helpful to explain the harm that rules are designed to prevent and protect against, and emphasise the ethical drivers for compliance.

Influencing behaviours is also a function of relationships at an individual level, and 'brand' at an organisational level. Anything that can help to establish one-to-one connections or improve the compliance team's visibility amongst those involved across the business can pay dividends. Hence, when appropriate, the example discussed above of replacing certain e-learning with face-to-face training can work on a number of levels.

It is also worth recognising that individuals can be disproportionately influenced by micro rewards. One of our favourite examples was an initiative to encourage employees

to adopt a clean desk policy and turn off monitors at night by occasionally doing the rounds after employees had left and leaving chocolates on the desks of those who had done so. Apparently this made a huge difference – and is a reminder of the need to balance the 'stick' with a bit of (chocolate) 'carrot'.

Ultimately, the business needs to understand the value that legal and compliance can bring. Legal and compliance teams are not there to be awkward or to make individuals' lives more difficult. Neither are they a safety blanket to replace good decision-making by the business.

A real indicator of the strength of a business' compliance culture is the degree to which it is self-policing.

Are you using the full toolkit?

There is no one-size-fits-all approach to compliance. Indeed, one of the most striking results coming out of our recent sessions was in answer to the question "who in your organisation takes the lead to manage compliance risk?"

In Bristol, the most popular answer (42%) was a Chief Compliance Officer (separate to the legal function). In London, the most popular answer (54%) was in-house counsel. In each location, there was a spread of answers that also included a Board member and a combination of the different functions.

Just as different organisations have different approaches to who takes overall responsibility, different organisations will have different risk profiles, geographical spreads, organisational structures and cultures.

Tech and innovation have an important role to offer, but are not the whole story. Deeper change can be effected by creating a culture that values compliance: nudge theory, internal brand-raising and individual psychology can all play a part in achieving this.

Compliance is an on-going, ever-changing challenge, with new tools and new risks being presented all the time. Things can still go wrong; but when they do, look for the opportunity amid the adversity to take your compliance function to the next level.

Katie Vickery
Chris Wrigley
Osborne Clarke LLP
katie.vickery@osborneclarke.com
chris.wrigley@osborneclarke.com