CAN THE CENTRE HOLD?

Regular columnist and risk expert **Annie Searle** ponders the global impact of recent high-profile risk events

Annie Searle

Annie Searle is a faculty lecturer at the University of Washington's Information School, where she teaches courses she designed on operational risk, ethics, policy and law as relevant to information technology. She is also principal of Annie Searle & Associates LLC, engaged in research and consulting through the ASA Institute of Risk and Innovation

"Turning and turning in the widening gyre
The falcon cannot hear the falconer;
Things fall apart; the centre cannot hold;"
William Butler Yeats, *The Second Coming* (1919)

These first three lines of a poem that Yeats wrote after the first world war resonate with us today and have been referenced in American political debate – and perhaps also around the Brexit vote as well. Going it alone or going it together with other countries appears at least to be the question as discord and violence present themselves more regularly, in no small part because of the technology now available to us.

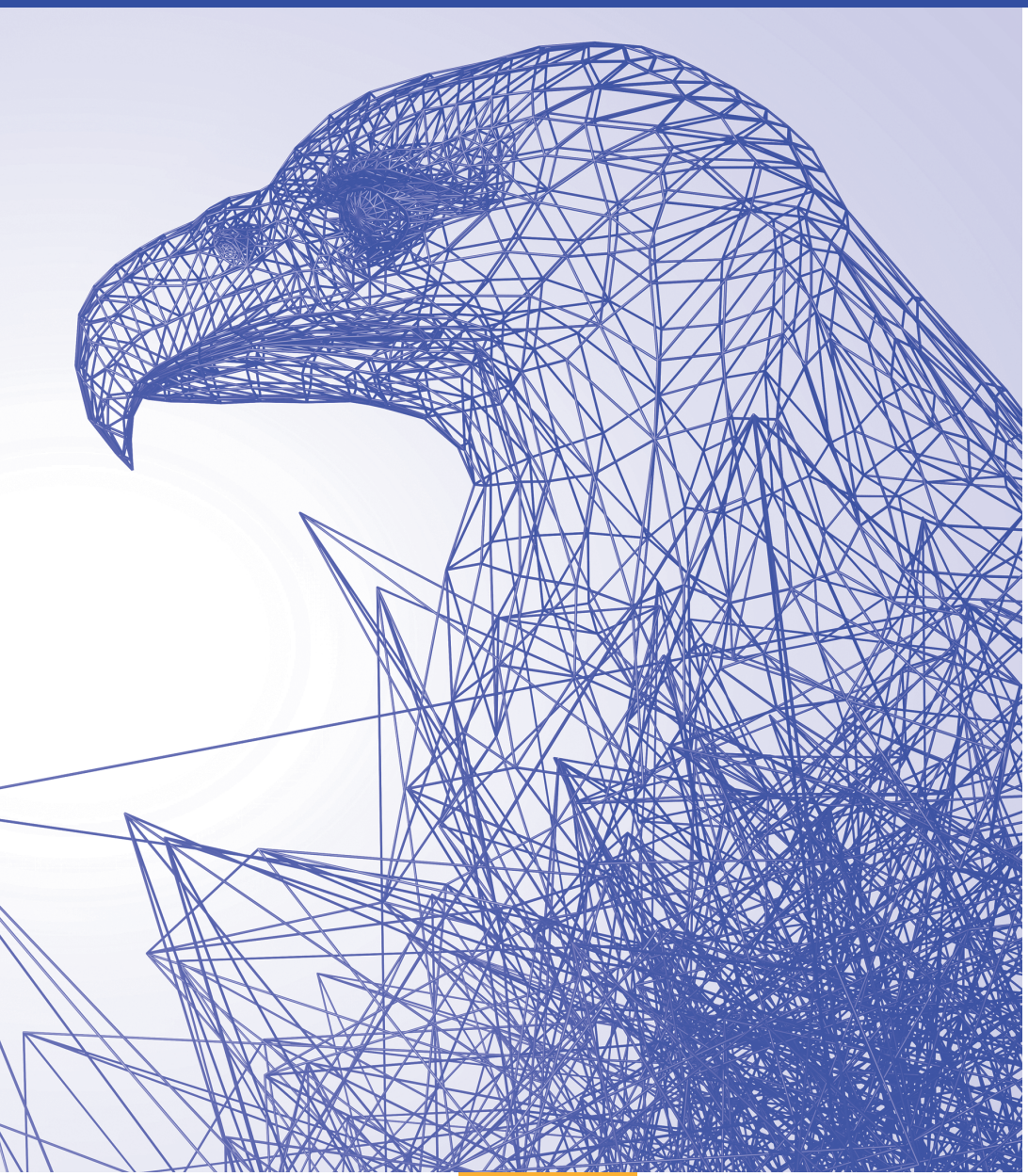
I've spent the past month writing about conduct risk, in particular about what I see as the top three root causes in banking: tone at the top; culture; and conflicts of interest. But as events continue to unfold, I see parallels in the real world, in particular around the two faces of technology, best illustrated by looking at some of those events.

In the world of cyber, two types of attacks appear pervasive: ones committed by nation-state players for objectives not always clear to us, but certainly to unsettle governments; and those committed by criminals driven by lucrative benefits around breaches, whether it's the sale of intellectual property, ransom demands to critical infrastructure firms, or the skimming off and sale of customer data.

Terrorism has added a frantic layer to our discussions. In this year alone, starting in March, suicide, active shooters and car bombings that had once occurred primarily in the Middle East moved into Europe and America again, starting with Brussels in March, then Orlando in June, then Germany and France again in July. At the same time, police in Dallas and New Orleans have been murdered, contributing further to the sense that things are out of control, that the centre will not hold.

Never before have international law enforcement officials been under so much pressure to reduce the incidence of unpredictable lone wolf attacks and to make communities safe once again for their citizens. More police departments are choosing to arm their officers with body cameras and, in some cases, with military body armour. At the same time, intelligence agencies like MI6 and the FBI are pursuing leads that point to both hackers and terrorists. Since the groups committing unspeakable acts are not traditionally organised and are, in more cases, self-radicalised from social media and other technology platforms, preventative or anticipatory intelligence efforts depend even more heavily upon technology, whether CCTV or active monitoring efforts of certain urban conclaves.

At the same time, privacy rules abroad are tightening, especially since the latest opinion by the



European Data Protection Supervisor. Here in the US, the FBI director has called for a robust discussion around encryption before the next terrorist event occurs; and, as indicated in an earlier column, the government's surveillance powers have been increased in both England and France. In the US, a whole political party has been taken over by a businessman whose rhetoric and careless promises remind us of earlier years in Germany and the rise of fascism.

What exactly can financial organisations do to keep their people safe and confident in their work, especially if based in France or Belgium – or even England? From our operational risk practices, we know that it is not possible to avoid all risk. But it is possible for firms to hold special training sessions for their employees that cover topics like active shooters and situational awareness. Some of this is common sense, but there are additional lessons to be learned from recent events. Firms may wish to harden their infrastructures even further and add a layer or two of physical security for employees. Business travellers should continue to expect delays, as governments determine what other measures they might put in place. Learning to be situationally aware is perhaps the next highest priority, especially if attending large public gatherings like sporting events, or parades, or other types of places where one must stand in line to enter. We know that terrorists have also effectively used public transportation systems and places of worship in addition to open air markets and restaurants.

Turning and turning in the widening gyre
The falcon cannot hear the falconer;
Things fall apart; the centre cannot hold

Visual scans of your environment for suspicious behaviour and/or packages is important. Being exhorted to be careful may be uncomfortable, but it is necessary. Just as we say "Think before you click" to employees about their email, "If you see something, say something" is a good mantra. There is always the possibility of hysterical finger-pointing. Efforts to remain calm and observational are hampered in both the US and Europe right now by the political rhetoric of fear-mongering. We have certainly seen some of that with air travellers in the US, who have insisted that certain passengers be removed if they speak another language or dress in their native garb. But I believe it's possible to settle in to practiced observation and reflection on what has become an uncertain world. Law enforcement alone cannot make us safe. We must do all that we can, together, to make the conditions in which we live and work less risky. In part, that means putting away our smartphones and looking about us with new eyes. Yes, that means being more careful – but it also offers an opportunity to see that for which we should be grateful every day. TRU