COSMOS
Navigate the Compliance Universe

Ethikos Volume 36, Number 3. July 02, 2022
Three Cs: Counterterrorism, counterespionage, and crisis management-Lessons for compliance

By Rupert Evill

Rupert Evill (rupert@ethicsinsight.co) is the founding director at Ethics Insight in Singapore and London.

Whatever area of risk and ethics and compliance (E&C) one is focused on, we all are broadly concerned with prevention, detection, and response. Counterterrorism requires precision in assessment, analysis, and communication that can help those of us working on preventive E&C measures. Counterespionage, by definition, fixates on detection and monitoring, posing some great questions and quandaries for us in E&C. Crisis management is the art of proportionate and effective response.

Having worked in each area in the past few decades, I'm starting to see where the different disciplines can help each other.

Counterterrorism class

Effective counterterrorism (CT) is multidimensional. We must consider several additional Cs: context, culture, capacity, and crown jewels.

Context

What is the operating context? In E&C, I sometimes see myopia around specific risk issues. We look to indexes to assess country-level corruption, money laundering, modern slavery, and sanctions. I would avoid such extractions at the national level. Your exposure is a function of what you do, where precisely in the country, whom you do it with, and how you do it.

For instance, a Texas-based biotech disruptor in the fertility space faces starkly different risks from a cryptocurrency platform in Manhattan. In CT, we're concerned with a broader basket of contextual indicators of risk. Political capacity, the rule of law, the efficacy of security forces, local-level demographics (including social issues), history, and conflict are all factors. I'm not suggesting that E&C professionals become country analysts for every single location of operation. This knowledge sits in the heads of your people—using around 20 E&C–specific country context questions (typically taking around four minutes to complete), we gather infinitely more insightful data than we do from indexes.

Culture

Next, we must understand the local culture. Whether your position is oppositional (looking for baddies) or capacity-building (hearts and minds), it's near impossible if you don't understand the societal, religious, cultural, and political dynamics at play.

For E&C culture analysis, we're most interested in knowledge, access, and trust. Are the compliance constructs understood by our audience? Conflicts of interests, gifts, hospitality and entertainment, and anti-competitive practices travel particularly poorly. Next, we should look at access to support (including leadership) and

resources. Many E&C failures occur when employees don't feel they can ask for help, admit they don't know what to do, or access advice quickly. Finally, we need to know whether people trust the leadership—and E&C. Trust is often more about perception than anything else. Do people feel leaders *walk the talk*, is everyone held equally accountable, and do employees feel leaders in faraway headquarters understand their frontline realities? Do they feel safe (nonretaliation, confidentiality, and anonymity) if they speak up?

I spent much of my career developing assets (i.e., human sources of information and intelligence). Asking people to tell you secrets or actively gathering intelligence in places where it can have severe consequences for life and liberty is a sobering endeavor. I sometimes see Northern European and North American E&C and leadership teams struggle to conceptualize that the *speaking truth to power* they hold sacred in their flat (and safer) hierarchies is almost entirely alien to others.

Finally, when we assess vulnerability in CT, we consider both security (controls) and predictability (culture). If terrorists know you go to the gym after dropping your kids off at school using the same route, your home fortress is rendered obsolete, and you're now an easy target for kidnapping. Similarly, in E&C, there can be a tendency to obsess about controls rather than the predictable (nonthinking and nonconscious) application of those steps. Where are you on autopilot?

Capacity and intent

When considering terrorist threats, we're concerned about capacity (capability) and intent. Not all threats are created equal. In E&C, we can assume that all threats are created equal. For example, corrupt demands are uniform.

An environmental inspector might cite (possibly spurious) violations in your facility that they're willing to overlook "for a small fee," or they'll hit you with a hefty fine (leveraging opaque regulations to their favor). A deputy minister furiously scrambling to buy votes for an impending election who threatens to cancel your operating license unless you pay millions is a different proposition. In this case, the minister's capacity is weak and their intent broad. Even in a very dysfunctional country, it's tricky taking a proposal to cancel a license generating massive revenue to your cabinet without a solid (quasi-)legal basis. My client was one of many targets for similar shotgun strategy shakedowns.

Again, there will be people in (and sometimes outside) your company who will know the unethical runners and riders. Qualifying the threat posed by external stakeholders—including (fair or capricious) regulators—will save time in the long term as you won't be doing the CT equivalent of assuming angry trolls pose similar risks as battle-trained insurgents.

Crown jewels

What do terrorists want? The answer depends on the terrorists' intent. If we know more about the intentions of external stakeholders, we have two tactical advantages: we know what to defend and how to negotiate. In the deputy minister example, the license cancellation required the approval of a local transport authority. Initially, the authority went along with the threats (bullets in the mail and alike). Still, if they canceled the license, it would significantly harm their reelection chances (in midterm equivalents). They'd previously campaigned on a go-green initiative and done nothing about it. My client implemented a raft of more sustainable changes (diesel to electric, renewable energy sources, and more). We then invited the local authority down to the unveiling of an upgraded facility, telling them they could take the photo opportunity and credit if they left us alone; they agreed.

As you map your security and predictability, spend the most time on your crown jewels. Next, consider what your higher-risk stakeholders consider your crown jewels—yes, cash will often be king, but not always. We can

often find ethical ways to appease challenging stakeholders.