KCS Group Europe

Corporate security: the ticking time bomb of in-house provision

July 2023

In-house intelligence teams are no longer fit for purpose in safeguarding their business' reputation and activities. Most of them lack the in-country experience and access to quality intelligence that is necessary for avoiding costly and embarrassing mistakes. Law firms, accountants and other businesses that rely solely on internal intelligence departments are playing a dangerous game in today's agile corporate environment. Stuart Poole-Robb, CEO of KCS Group Europe (KCSGE), has a stark warning for governments and businesses: *'You're operating in a minefield. You need quality intelligence and accurately assessed, assured information to help you navigate safely.'*

Think discreet intelligence professionals who separate fact from fiction, who protect clients from misleading and manipulating noise, and who provide accurate, relevant information about current risks and threats. Most in-house intelligence departments do not have the expertise and resources, leaving their businesses vulnerable to error and exploitation. For example:

1. A client was intent on maintaining a partnership with a business in Eastern Europe, until a specialist team from KCSGE uncovered confidential, incriminating intelligence about the key stakeholders.

2. Eleventh-hour intelligence provided by KCSGE revealed that a potential partner was looking to use a UK firm and its reputation to launder stolen money. The client was saved from embarking on activities that would have proved very costly, illegal and embarrassing.

Businesses need access to cutting-edge analytical software and strategic human assets on the ground. They need long-term, in-country experience and knowledge of key individuals. They need information that is not in the public domain. It is only external agencies that can provide intelligence of the breadth and depth required by today's corporate entities.

Key risks and threats

Businesses and governments can, of course, identify many of the risks that threaten their activities. But the sophistication of today's cyberthreats, security risks, economic downturns and situations of political instability is beyond most in-house teams.

Cyberthreats: The notorious 'Worm' virus of the 1990s has morphed into unassisted AI bots that keep rewriting themselves until they break down IT defences. The ensuing costs – both financial and reputational – can be catastrophic and embarrassing.

Security risks: Methods of gaining unauthorised access, undertaking theft, espionage or physical harm continuously shift and evolve. Experience across different sectors, familiarity with historic and current trends and an ability to identify potential negative outcomes is needed.

Economic downturns: Businesses need effective monitoring of market movements and trends that allow them to accommodate negative trading conditions. Swift identification of downturns but also of valuable opportunities can help them thrive even in the face of challenging circumstances.

Political instability: Worldwide monitoring of geopolitical factors, social unrest, local government policy and environmental hazards is vital to alert businesses to emerging threats that are relevant to their investments and strategy.

Nationally and internationally, the CIA, MI6 and Mossad keep track of bad actors and fluid landscapes in order to mitigate risk, limit damage and protect business and personnel interests for their governments. The private sector cannot afford to be any less meticulous. Businesses must match the vigilance of national governments and carry out their operations with credible, relevant intelligence. Most cannot do this without the assistance of external, in-country support.

Ethical considerations

Many prominent organisations have significant resources at their disposal, allowing them to conduct their own covert enquiries. But sometimes, they fall foul of the law or ethical considerations. Credit Suisse, for example, came up against severe criticism in 2020 for the way that its CEO, Tidjane Thiam, hired private detectives to spy on his former head of wealth management after he left for a rival firm. There were several other allegations of spying operations conducted by Credit Suisse between 2016 and 2019. Specialist, external providers such as KCSGE adhere to moral, ethical and legal use of intelligence.

What makes a good intelligence professional?

A strong analytical ability, a passion for critical thinking and problem-solving are key. A sound ability to collate and assess data from both open source and classified sources and communicate it effectively verbally and in writing. A knowledge of counterintelligence, geopolitical analysis, cybersecurity and counterterrorism. Skills in search methods and tools used for presenting complex data, data mining, monitoring social media, geospatial analysis and secure VPN communication. An external agency can bring these skills to a business or government department – or supplement the skills of an in-house team.

Andrew Beurschgens of Strategic and Competitive Intelligence Professionals notes: *'Today's businesses … operate in an increasingly VUCA world; that is, in a world characterised by Volatility, Uncertainty, Complexity and Ambiguity.'* The only viable strategy is to make decisions based on the ethical and legal collection and analysis of information which must be assessed by four Vs: its volume, variety, velocity and veracity. *'This is best achieved by a dedicated organisational function'* and *'the ideal antidote to the VUCA world.'*

A dedicated intelligence team – whether it's internal or outsourced – is not an act of corporate vanity. It is a fundamental aspect of governments' or businesses' Risk Radar, proven to protect the bottom line.