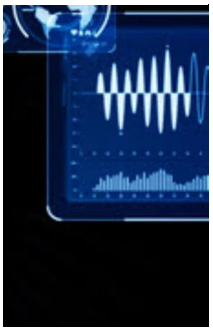

SHARE (https://www.linkedin.com/sharing/share-offsite/?url=https://www.hcgroup.global/hc-insider/insights/the-future-of-trade-surveillance) (https://twitter.com/intent/tweet?https://www.hcgroup.global/hc-insider/insights/the-future-of-trade-surveillance) (http://www.facebook.com/share.php?u=https://www.hcgroup.global/hc-insider/insights/the-future-of-trade-surveillance)

INSIGHTS

The future of trade surveillance

HC INSIDER Financial Services • 5 min read • 08 September 2021

Surveillance is a key requirement for trading firms to improve risk detection, identify market abuse, and address offences. HC Insider speaks to Alan Lovell, CBE, ex-Managing Director, Global Head of Surveillance, HSBC, to better understand best practice in trading and communications surveillance, including in the energy markets.

Human Capital has partnered with intelligence provider 1LOD to become an Associate Sponsor for the Energy Trading Surveillance Deep Dive (https://www.1lod.com/deep-dives/energy-trading-surveillance-deep-dive) event on 14 and 15 September. At the event, senior surveillance and compliance leaders, along with regulators, will debate best practice in trading and communications surveillance for the energy markets. HC Insider speaks to keynote speaker, Alan Lovell, CBE, ex-Managing Director, Global Head of Surveillance, HSBC, to find out how the surveillance landscape is changing and what this means for trading firms.

HC Insider: What are the types of market abuse affecting energy firms?

Alan Lovell: The market abuse risks that affect energy firms are broadly equivalent to those that apply to other products across the financial sector, and firms generally settle on a market abuse risk taxonomy – the set of technical market abuse scenarios that the firm decides it wants to mitigate. Examples of market abuse that particularly concern regulators would include front running a client's order on the basis of non-public information, or the market manipulation of an energy product benchmark. Across the many technical trading scenarios in which traders might seek to influence the price of a commodity, discerning the motivation and intent of a trader can be a nuanced challenge. A core point for the effective management of market abuse risk is that the risks are dynamic – they evolve as trading activity evolves. Horizon scanning for emerging risks is essential, as is the continuous review of whether existing controls can still detect the risks they were created to mitigate as trading practices evolve.

HC Insider: What are the global regulatory expectations on energy firms to mitigate market abuse?

AL: Different regulatory jurisdictions have different priorities, but I think market abuse in its many forms remains high on the agenda, regardless of the product being traded. The EU's 2016 Market Abuse Regulation, on shored into UK law at the end of 2020, is definitive on the subject. Also, US regulators have sent a clear global message that they will not tolerate market abuse and will seek to prosecute where they can. There are other heavily-regulated risks in the financial crime space, such as money laundering and fraud, but the message is clear – the onus is on organisations to understand and mitigate the risks.

HC Insider: Should energy trading businesses be buying or building their surveillance technologies?

AL: This is a difficult question to answer generically because it depends on your in-house technical capability. Some organisations have a fair chance of achieving it in-house, some not. From my perspective, if you're going to do it in-house, then you need a very capable tech department that won't be side-tracked by other projects or unnecessary functionality, and you need a reliable funding stream. I've seen some businesses change their plans mid-project because of wider changing priorities, which dilutes first line confidence and trust in the project. I think some people often presume that keeping the capability in-house will be cheaper. In many cases it would probably be best to buy the surveillance technologies because then the business benefits from an upfront understanding of the costs and functionality. Another factor when determining whether to buy or build, is the company's appetite for risk. It's important to protect markets and your reputation, and not just the bottom line.

HC Insider: How much should energy trading businesses be spending on their surveillance capabilities?

AL: It depends on the organisation's risk appetite and the path they choose to follow regarding technology. Surveillance is not just an add-on – it's a core element in an organisation's wider conduct efforts and their ability not just to detect bad behaviour but to enrich the organisation's understanding of its staff's motivations and its performance. Surveillance can be a tool to mitigate reputational and economic risk, but also assist in the development of an improved, more productive, higher-performing work environment. Companies should invest seriously in this and it's not going to be cheap if approached properly. There is the temptation to under-invest, to change direction mid-programme, particularly in volatile economic circumstances.

> "Organisations should migrate to a risk-based approach, aiming

HC Insider: What is the difference between a rules based and an integrated risk based approach to surveillance?

AL: The rules-based approach seeks to reduce a wide range of trading scenarios to a set of simple rules which, when triggered, alert surveillance staff to potential market abuse. Given the scope and complexity of trading activities, and the often-arcane language traders use when conducting them, the result is a plethora of rules – a haystack in which we need to find the needle, essentially by examining each piece of hay. Each alert is treated as of equal concern until a human has assessed it. The result is a need for large numbers of staff to work through alerts, most of which are false positives. It is expensive, not very effective, and uninspiring work. A risk-based approach seeks to use technology to identify true positives more efficiently and to attach some priority to them with the aim of ensuring that staff are guided to what matters most first.

HC Insider: How should trading organisations migrate from rules to a risk-based approach when it comes to surveillance?

AL: Organisations should migrate to a risk-based approach, aiming to use technology to identify the riskiest activity or person first. It means you mitigate the worst risks faster, and arguably you keep the organisation safer. It requires surveillance staff to work on a prioritised list of threats and although they will rarely make it all the way to the bottom of the list, they will at least continue to focus on new, higher-level risks. In my opinion, this is the only viable way of genuinely staying on top of dynamic risk situations while maintaining a viable cost profile. This is an uncomfortable position for a risk manager in a commercial organisation to take and they will wonder how they can migrate from a rules-based method to a risk-based approach. Generally, there will be a period of time where you are running both approaches, which is expensive, but you will be able to retrain some of your rules-based staff on the new risk-based equipment. So, the cost profile goes up before it eventually comes down.

HC Insider: Have compliance functions got the right people with the right understanding of the energy markets in place to conduct effective surveillance?

AL: I can't speak for all companies engaged in energy trading, but professional compliance officers, who have historically been the backbone of surveillance efforts, have invaluable skills. Their diligent application of processes and their understanding of the regulatory landscape is absolutely essential. But surveillance also requires deep insight into the particular products that are being traded and how they're being traded, and that understanding needs to be dynamic and you need to keep up with new methods, new jargon, and new trading systems. The act of analysing and assessing technical and behavioural risks that the detection systems produce is an art in itself, which is why at HSBC I enriched my compliance-heavy surveillance teams with ex-traders and staff with investigative and analytical skills from outside the financial sector. In my experience, diverse teams that work together to discuss and assess risks are more productive.

HC Insider: What are the privacy and data privacy concerns surveillance functions should be concerned with?

Alan Lovell: Comms surveillance is one of the most intrusive activities that any organisation can engage in. You're basically looking at all of your staff's intimate comms. This is why when governments engage in such activity (for example for law enforcement) they have approval systems in place for such capabilities that generally require ministerial sign-off. Being charged with the job of probing into the communications of colleagues is a big responsibility that requires appropriate management procedures, checks, and balances, and good, continuous training. Data generated by trading companies is self-evidently highly commercially sensitive and needs to be well-protected. Many organisations are on a path to moving their data to the cloud.

HC Insider: How can surveillance functions reduce the number of false positives picked up by their surveillance systems?

AL: Fundamentally, as well as strict curating of existing lexicons and other controls, what the surveillance operator needs is context and the training to use that contextual information to make better, faster decisions. The aim should be to have as much relevant and accurate information as possible readily available to users from a range of detection systems, along with other behavioural information about trading staff. The surveillance of trading staff is, in my view, a subset of the wider internal risk efforts of the organisation – risks associated with internal fraud, disciplinary issues, data leakage for example – and should be integrated with them.

HC Insider: What will surveillance functions look like in five to 10 years' time?

AL: Five to ten years ago, people were concluding that an integrated holistic picture was necessary. They were already deciding that rules-based systems were inefficient, costly and an inadequate approach to risk mitigation. Back then, AI was emerging as the concept du jour, though its application in this field was not well understood. Cloud-based archiving was something that most companies had yet to engage in. I think we can all now see that the hill we have to climb is steeper than we first imagined and there is no cheap solution. New trading platforms have come along, many of them with an embedded chat function. In addition to this, volatile markets and the pandemic are all challenges that need to be overcome. But we are seeing some tech surveillance products emerging that are integrating the different detection streams, and some organisations are becoming more comfortable with a risk-based approach. I'm optimistic that an integrated risk-based approach which benefits from advanced language processing and machine learning, as well as more nuanced algorithms for contextualising trading activity, will be the norm within the next five to 10 years. The pace, however, will depend on each company's appetite to grasp the nettle and for technology providers to respond imaginatively to industry needs.

For your chance to hear Alan speak at the Energy Trading Surveillance Deep Dive event, taking place on 14 & 15 September, book your place here (https://www.1lod.com/deep-dives/energy-trading-surveillance-deep-dive#Book%20Tickets) or contact Dane.Barnard@1lod.com.

Download the agenda for more information. (https://mcusercontent.com/75af0d55592fa444243aa030b/files/bc879f0c-f116-a8e9-734c-cf3ff1dc6c10/Energy_Trading_Surveillance_Working_Agenda_010721.pdf)

Related Consultants