The Surveillance Leaders Network

FORECAST 2022

smarsh® 1LoD®

Surveillance moves to the top of the risk agenda

"As an industry, we share the same goal of effective detection of market misconduct risk behaviours so that we can better serve our customer and clients and drive fair market. The Surveillance Leaders Network allows this dialogue to happen and drive this common goal."

- **CHUANG YI**, MANAGING DIRECTOR, SURVEILLANCE TESTING EXECUTIVE, BANK OF AMERICA

E-comms surveillance tops the list of priorities for enterprise risk management, according to participants in 1LoD's recent in-person Surveillance Leaders Network in New York. Leaders asked the obvious question: if electronic communications are listed on a firm-wide risk register as part of its enterprise risk control framework, shouldn't the resources allocated to manage that risk be increased?

Other key topics for discussion included:

Data capture risk must be treated as separate from pure surveillance risk because regulators demand multi-channel coverage: The 'surveillance surface' has increased over the last two years and regulators now take a tougher stance. It is imperative to capture new channels and ensure that the capture-index-archive process satisfies regulators across the pool of regulated employees. Smart analytics of those channels must wait. Banks which have resisted adopting capture solutions that do not encompass all of their current and future needs – and that includes some of the largest institutions – may have to think again.

Broader RCSAs must be supplemented by rigorous surveillance risk assessments: "Any good surveillance programme should of course be predicated off a fully traceable risk assessment. This is one of the first things that any auditor/examiner will tend to ask us in terms of explaining our coverage and how we are able to track back our coverage, or indeed our book of work to the underlying risk assessment process," says one surveillance leader. RCSAs (risk and control self-assessments) are too broad to capture granular issues in surveillance, and SRAs (surveillance risk assessments) are needed to fill the gaps. "Should you be doing your surveillance risk assessment from a product perspective or a business unit perspective?", asks another surveillance head. "Typically for us the RCSA is more of a business unit, desk-led exercise; the surveillance risk assessment is done from a product perspective, because we build surveillance specific to products."

Surveillance needs to respond more quickly to business change: Divergence from traditional market behaviours – the rise of the retail meme investor, venues such as Reddit as potential tools of market manipulation, crypto – is a challenge and, "changes things in terms of risks and what to look for in our own traders. Different language is being used, so we need to look for that, and then we need to think about short squeezes by retail crowds and the concept of market manipulation itself when applied to coins like Bitcoin." This means it is critical to keep up to date with the business more regularly than with the annual SRA engagement.

New product approvals processes should embed an evaluation of their surveillance consequences: Some leading banks have moved to a model where it is now a requirement to assess the surveillance consequences of a product during the development process of that new product, pre-empting potential issues. This also makes the annual SRA easier because it can be partially created by combining these 'mini' assessments and adding them to the existing baseline.

Incorporating trade data into e-comms surveillance is the right strategy: But surveillance leaders disagree over whether this improves or increases false positives and noise. There is also more work to be done in using AI (artificial intelligence) to organise unstructured data so that this aggregation is easier and more effective. However, one question is whether AI should be used first, to prioritise alerts for review after they have been generated.

Broader behavioural analytics are accepted as a key tool in the future of surveillance: More banks want to combine rules-based with behavioural analysis but there are still many different definitions of the term. Some of these require risk scoring individuals, which is controversial, especially if it includes the use of HR and other data in combination with surveillance data. Others entail AI-assisted pattern detection or network analysis to spot anomalous behaviours more generally across larger groups. And plenty still worry that the regulators are happier with simple lexicon- based sampling because although it is ineffective, at least it can be explained.

This information was taken from the Surveillance Leaders Network event in New York, June 2022.

CHART 1

Chart 1: My firm has implemented a comprehensive Surveillance Risk Assessment (SRA):

- ○ Fully
- ● Partially
- ● Minimally

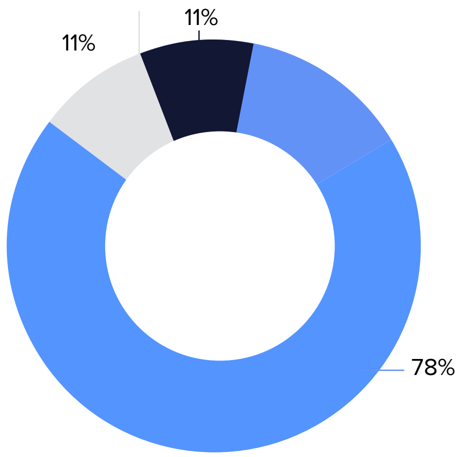
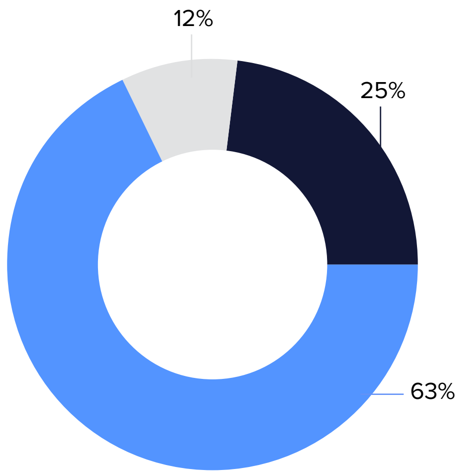


CHART 2

My organisation has moved its conduct surveillance from analysing market abuse surveillance alerts to wide-ranging metadata analytics using machine learning:

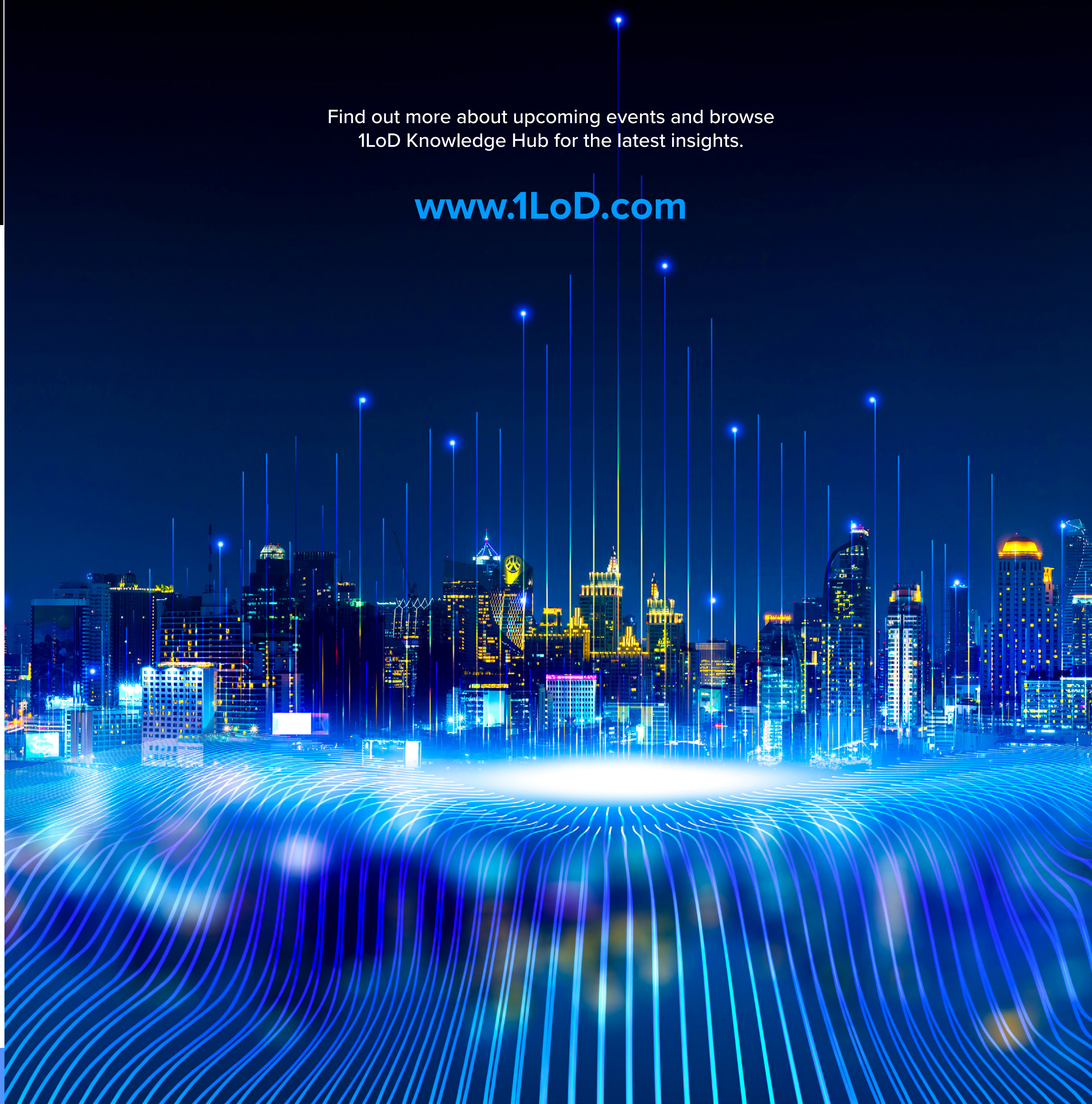
- ○ Yes
- ● Partially, we are on a journey
- ● No



> *"The Surveillance Leaders Network is a great forum to discuss key industry topics with peer groups which can only further the development of common best practise."*
>
> *RICKY CRUMP, HEAD OF TRADE & COMMUNICATION SURVEILLANCE, DANSKE BANK*

smarsh®

1LoD®



Find out more about upcoming events and browse 1LoD Knowledge Hub for the latest insights.

www.1LoD.com