blackdot
solutions

Open Source Intelligence: Transforming Financial Crime Investigations

By Matthew Redhead

Executive Summary

- 'Intelligence' material has long been seen as secret information which requires covert measures to collect. But in reality, intelligence is any material that can provide insights to a given consumer.
- With the growth of the Internet and other technologies, the full range of what can be considered as intelligence has become increasingly apparent. The value of 'Open-Source Intelligence' (OSINT) to intelligence professionals has increased as a result.
- OSINT has also seen increased usage in those parts of the private sector that require rich contextual intelligence to make risk decisions. Multinational businesses with interests in emerging markets are common examples.
- OSINT has been used in client-facing parts of the financial services sector, but less so in financial crime compliance and risk management. Here, there has been a tendency to privilege insights from internally collected transactions and client data.
- This picture has changed recently, however, with growing numbers of compliance and risk functions finding ways to exploit OSINT: most commonly enhancing pre-existing compliance processes, but also supporting new, proactive intelligence operations.
- In both cases, OSINT has added value, but challenges remain. Many continue to rely on Internet-based search strategies that are little more effective than 'prospecting for gold'.
- The response to this challenge is the use of tailored OSINT solutions: ones providing access not only to large amounts of information, but the most germane material, relevant to the needs of the client.

Introduction

In the last forty years, major businesses have begun to see much of the material they possess as a form of 'intelligence'; in other words, information or data that can reveal insights about their customers, their products and the markets in which they operate.

In the financial services sector, the use of such 'commercial' or 'business' intelligence has been most common in the front office, driving the exploitation of new opportunities. The concept has also caught on in risk functions too, and latterly financial crime compliance and risk management departments.

After facing a succession of bruising regulatory fines, many such departments have asked themselves whether they too might take an intelligence-led approach. In an increasing number of cases, 'financial crime risk intelligence', has become an important way of identifying and mitigating those risks – while also sending positive messages to the regulator about the institution's ethos and intentions.

There has been some bias so far towards using only the information an institution already has at its disposal, such as static customer information or transactions data. However, other institutions have found additional benefit through the application of OSINT alongside proprietary material.

At its most fundamental, this has involved the blending of OSINT into core compliance and risk management activities, to ensure that operational decision-making is based on a broad and rich intelligence landscape. But in more innovative cases, businesses have sought to re-shape reactive 'compliance' processes into a more proactive, intelligence-led framework, in which OSINT can play a central role.

This paper seeks to explore the concept and value of OSINT, and look at how it is already helping compliance and risk professionals fight financial crime more effectively. It also seeks to take an honest look at the challenges that come with using OSINT, especially given the deluge of material now available, and points towards ways in which technology can help financial institutions generate a greater dividend from OSINT.

Defining 'OSINT'

The meaning of 'intelligence' has been a challenge for practitioners and scholars of the field alike since the first formal government intelligence agencies began to appear just over a hundred years ago. Most of those who have attempted to create a definition have tended to focus on the clandestine nature of state agencies' work, seeing intelligence as the collection of opponents' secrets through the use of secret means, such as human sources or the interception of communications.

But thinking of intelligence as something inherently clandestine is restrictive and arguably inaccurate. At foundation, the idea of intelligence has always been that it is more than just inert information – the key ingredient being that it has exploitable value for the person or organisation collecting it. This means that, within reason, just about any kind of information can be 'intelligence' in the right context, regardless of how mundane that information is, or how it has been collected. For instance, online reviews of local restaurants will not only be of use to a relatively small number of diners in the area, but also to potential entrepreneurs or national restaurant chains seeking to expand. It is clearly 'open source', and it is also – for businesses making strategic decisions – very useful indeed.

This suggests that the idea of OSINT – although coined only relatively recently – has always been a fundamental part of what intelligence is about. So why are we talking about it so much more now? Almost certainly, the answer comes from the explosion of data and information that has become available as a result of the creation of the Internet and the development of cloud computing, which has allowed users to store, analyse and access vast amounts of disparate material through distributed global networks. According to the online statistical database 'Statista', the total amount of data created, captured, copied, and consumed globally is growing at a dramatic rate, reaching 64.2 zettabytes in 2020, and projected to grow to more than 180 zettabytes in 2025. Indeed, in 2020, the amount of data created and replicated reached a new high because of increased use of online and mobile technologies as a result of the social restrictions following the onset of the COVID-19 pandemic.

> One zettabyte is equal to one sextillion bytes or 1021 (1,000,000,000,000,000,000,000) bytes. See https://www.statista.com/statistics/871513/worldwide-data-created/ for further details of data growth.

With the growth in volume of online information over the last thirty years, the concept of OSINT has been able to take on a meaning and potential impact it did not have before. In the past, open-source material was mostly limited to printed media, such as books, articles, public records, etc, that could usually only be viewed at specific places and times. Now, however, the existence of the internet has meant that users can not only access published materials with relative ease, but also self-published blogs, social media posts, and a whole range of visual and auditory media that either did not exist prior to the development of smart phones and mobile technology. In many ways, the Information Age is also proving to be the Age of OSINT.

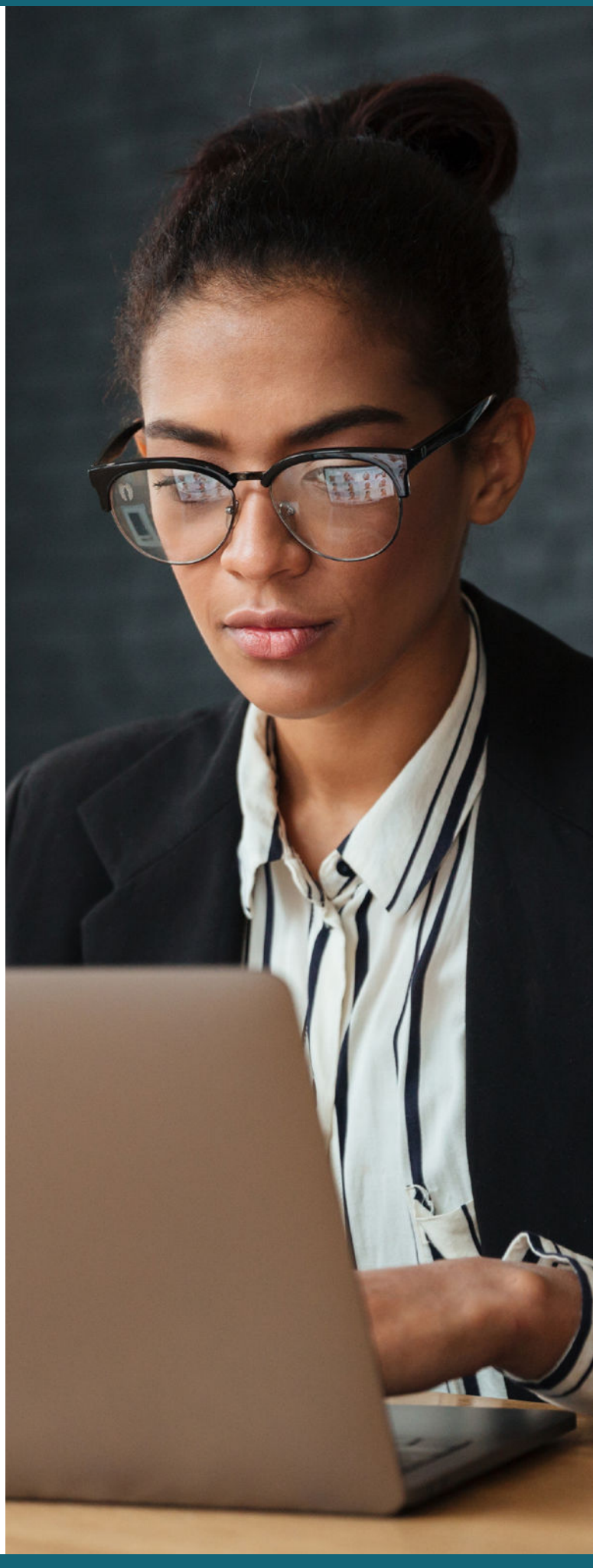
At its most fundamental, this has involved the blending of OSINT into core compliance and risk management activities, to ensure that operational decision-making is based on a broad and rich intelligence landscape. But in more innovative cases, businesses have sought to re-shape reactive 'compliance' processes into a more proactive, intelligence-led framework, in which OSINT can play a central role.

This paper seeks to explore the concept and value of OSINT, and look at how it is already helping compliance and risk professionals fight financial crime more effectively. It also seeks to take an honest look at the challenges that come with using OSINT, especially given the deluge of material now available, and points towards ways in which technology can help financial institutions generate a greater dividend from OSINT.

Who Uses OSINT?

Forward-thinking organisations have thus been seeking to tap into the potential of OSINT to help them achieve a better understanding of their operating environments. Government agencies – previously the bastions of the conventional wisdom that 'intelligence = secrecy' now take OSINT much more seriously. In March 2005, the US 'Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction' found that amongst the mistakes made by the US intelligence community over the identification of Iraqi Weapons of Mass Destruction (WMD) programmes, was a failure to use OSINT effectively to expand, enrich and challenge secretly collected materials. As a result, the then Director of National Intelligence (DNI), John Negroponte, created a new, independent US OSINT agency, now called the National Open Source Enterprise.

Beyond the secret world, the variety of open-source material now available has also enabled the development of new forms of almost 'crowd-sourced' investigative journalism. Online groups such as the Organized Crime and Corruption Reporting Project (OCCRP) and the International Consortium of Investigative Journalists (ICIJ) have been able to combine leads developed via classic journalistic techniques with publicly available information to crack and develop major stories such as the discovery of large-scale money laundering through Scandinavian, Baltic and other European banks. In the business world too, major multinational firms operating in high-risk jurisdictions and emerging markets – for example those trading in oil, gas, commodities or pharmaceuticals – have taken a deep interest in the potential of OSINT to provide them with a rounded view of risks and issues as they make decisions about new operations in potentially challenging locations.



OSINT in Banks

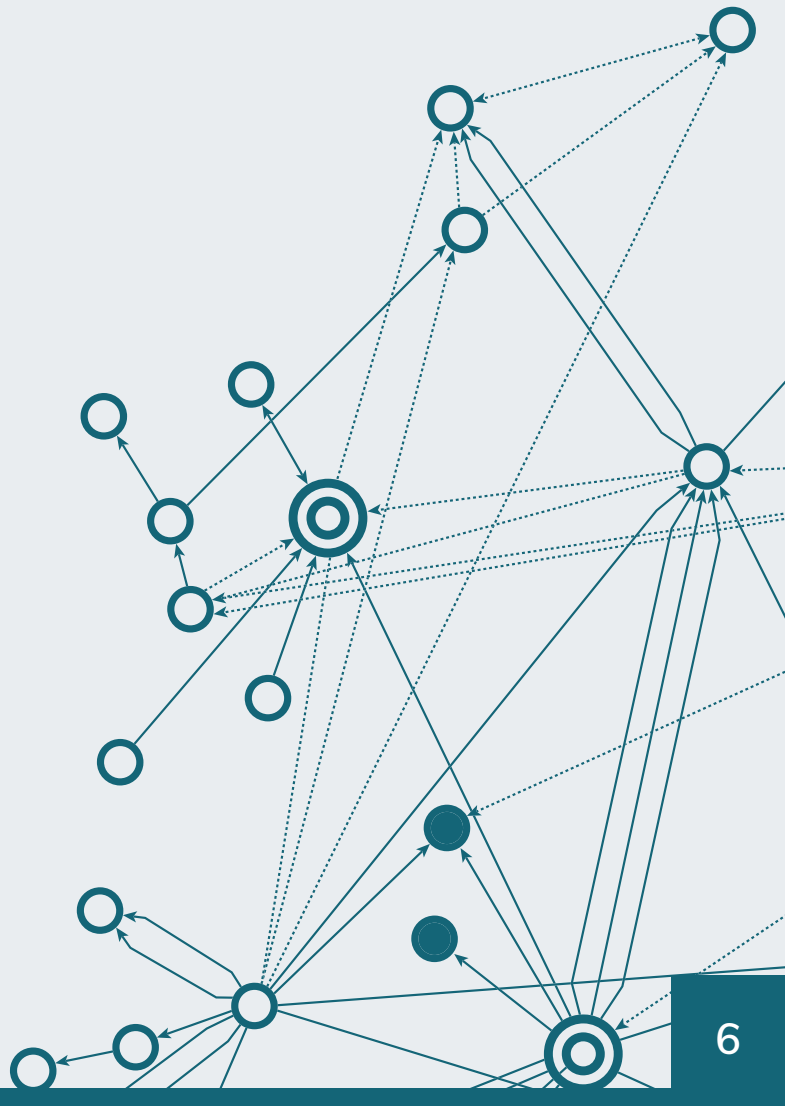
Although the acceptance and usage of OSINT has progressed in many risk-focused parts of the public and private sector, it has taken a little longer to be embraced fully across all dimensions of the financial services. This has not been a universal situation, of course. As noted in the introduction, some front-offices in larger financial institutions have become adept at the use of intelligence, including OSINT, in commercial decision-making. Since the 1980s, financial institutions have hired boutique risk consultancies to undertake Enhanced Due Diligence (EDD) on clients and potential clients in emerging markets. Some financial institutions have also developed their own in-house intelligence teams to do the same. In both cases – and despite what some of their more romantic clients might wish to think – such teams make extensive use of OSINT in their research strategies.

In comparison, however, financial crime compliance and risk management functions have been more cautious about using OSINT in a systematic way. This has not been out of any hostility to the concept of course, but more because it has not been necessary under the basic regulations of Anti-Money Laundering and Counter-Terrorist Finance (AML/CTF). In most cases of Customer Due Diligence (CDD), financial institutions have only been required to make judgements based on the data they have in front of them – whether that be customer documents or the patterns of account behaviour – rather than go out of their way to collate further material. The major exception to this, of course, have been those cases which have required EDD or other forms of investigation, but these have usually been a small minority.

A Changing View?

The perception of OSINT as marginal to compliance and risk management remains common in some financial institutions, but interestingly, not all. Several have been looking again at the potential of OSINT to help them assess and act upon potential financial crime and reputational risks, for example increasing interest in OSINT-specific training courses and technologies designed to exploit publicly available information.

There are several reasons for this shift. In many cases, the institutions that have chosen to innovate have done so after facing major regulatory fines for failings around financial crime compliance. Like the US intelligence community after the Iraq WMD debacle, they have come to realise that there is valuable intelligence available in their midst, to which they were not paying sufficient attention. This has been a point that has also been emphasised by the waves of law enforcement, military and intelligence professionals that have moved into financial crime compliance and risk functions since 2010. Having learned the lessons themselves before, many intelligence professionals now working in the private sector have wished to ensure that their new employers do not make similar mistakes



Enriching Compliance

Amongst those compliance and risk management functions that have started to take OSINT more seriously, there has been a common pattern of seeking to enrich pre-existing processes with the use of open-source material. Although AML/CTF laws and regulations place many obligations and responsibilities on firms, these largely resolve down to two key concerns – prevention and detection. It is the firm's responsibility to ensure that it prevents known or suspected criminals from misusing their products, and thus the wider financial system, as well as having effective monitoring and reporting mechanisms in place if they slip through the net. As is obvious, there is a natural dovetailing here between the needs of the financial institution and the benefits that OSINT can offer, and as a result there are numerous places within a typical financial crime function that it can and has been deployed. Some of the most common examples include:

- **Onboarding:** During Identification and Verification (ID&V) and CDD measures for individuals, and Know Your Customer (KYC) checks for business clients, some financial institutions are now proactively cross-referencing client-provided material with OSINT, going beyond the requirements of EDD for 'high risk' clients such as Politically Exposed Persons (PEPs). In these instances, credible OSINT can prove a useful corrective or complement to the information provided by a client or found in standard sanctions screening or watchlists. But it is worth remembering that these lists cannot contain all hostile actors, meaning that broader access to OSINT is necessary if an organisation wishes to effectively identify risk. In business relationships, OSINT is also playing a vital role in understanding a business's purpose when undertaking 'Know Your Customer's Customer' (KYCC) checks.
- **Client Reviews and Remediation:** CDD/KYC teams also exploit OSINT not only in regular client reviews, but also larger scale remediation projects looking at particularly risky client sectors, such as correspondent banks or Money Service Bureaus (MSBs).
- **Platform Alerts and Event-Driven Reviews:** Typically, sanctions screening and transaction monitoring alerts are analysed using spreadsheets or basic social networking tools. But increasingly, financial institutions are equipping their analysts and investigators with OSINT tools to help them flesh out potential risks, and provide more helpful detail in sanctions breach reports or Suspicious Activity Reports (SARs).

It is also worth noting that OSINT has increasingly played a role in the management of adjacent risks to financial crime, such as reputational and geopolitical risk, as well as broader commercial processes, such as Vendor Risk Management (VRM). For example, with increasing concerns amongst banks about exposure to clients linked to wildlife and environmental crimes, or human trafficking and modern slavery, OSINT has played an increasing role in testing the veracity of suppliers' claims to be acting legally and ethically.

Transforming Financial Intelligence

In the first instance, therefore, OSINT is helping some financial institutions undertake their core financial crime compliance obligations with greater effectiveness and assurance than before; OSINT is helping anti-financial crime functions to reduce the dangers of 'flying blind' in an ever-more complex environment.

Nonetheless, in the most advanced firms, OSINT is playing a further role in the transformation of how financial crime risks are managed. As noted above, new thinking over the last decade has started to reverse the traditional compliance-led, 'tick box' approach, towards a 'next generation' strategy that makes financial institutions proactive participants in the fight against financial crime (see our AML Investigator Revolution). This has involved the introduction of integrated investigative teams within financial crime functions, as well as internal Financial Intelligence Units (FIUs) and risk analytics teams, intended to develop operational and strategic views of financial crime risk, beyond the day-to-day tactical concerns.

In these newer teams, OSINT has been playing an essential part in helping develop more detailed views of clients, wider networks and associations, combining traditional internal 'financial intelligence' or 'FININT' – especially transactions data – with OSINT material. In several cases, this approach has helped not only identify unknown risks related to classic financial crime typologies and behaviours, but unearth complex emerging risks from networks involved in multiple forms of predicate and financial crimes.

Being able to find these previously unknown risks has placed senior staff in a stronger position to make informed decisions, and has also aided the development of investigative relationships with law enforcement through the production of better SARs. Law enforcement officials interviewed for the Royal United Services Institute (RUSI) paper Deep Impact in 2019 noted that financial institutions using the most innovative approaches, including more systematic exploitation of OSINT, are providing better intelligence material for law enforcement agencies than before.

And although the main point of this approach is not simply to please the regulators, it is absolutely vital that responsible financial institutions demonstrate the use of the full range of available intelligence where there are high risks, and Enhanced Due Diligence (EDD) is required. Regulators are unlikely to be impressed with a business's failure to use OSINT effectively in such situations, and businesses are running a regulatory risk if they do not do so. The deployment of OSINT not only enhances existing processes therefore, while also providing additional layers of monitoring and coverage, but evidences to regulators the institution's thorough application of the Risk-Based Approach (RBA).

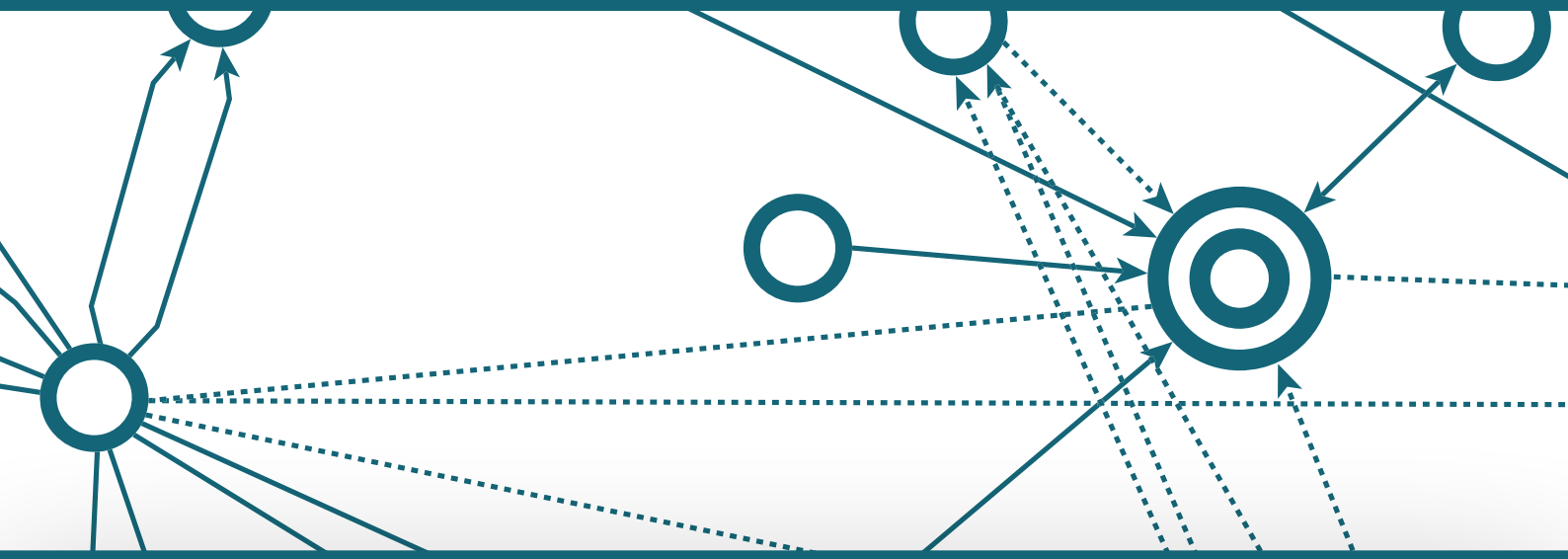
OSINT Challenges

The use of OSINT does not come without challenges, however, and some of these are being exacerbated by the ways in which financial institutions are choosing to source and manage the material. Unfortunately, many firms are using the most inefficient means at their disposal – unmediated and often unsystematic searches of the Internet through common search engines.

This is far from being an optimal strategy, for good reasons that are now more widely understood than in the early days of the internet. Analyst-defined searches, even where the intelligent use of keywords and strings are applied, are likely to miss much material, because of the underlying parameters of the search engine and the IP address from where the search is conducted. If you are in the UK searching for material on a firm or individual in China, you are unlikely to get the best information available. Similarly, the output of a search is shaped and prioritised by the past search behaviours of the user, meaning that engines have a predilection for serving up to you what it thinks you wish to see, rather than what you need to see. Despite the current popularity of OSINT training courses, it is worth remembering there is absolutely nothing such courses can do to deal with this kind of problem. The bias is built-in.

On top of this, search engine-based collection of OSINT faces other fundamental challenges of selection, assessment and security. Search engines will typically deliver vast amounts of sites for analyst review, making it difficult to know where the appropriate 'cut-off' point should be. Analysts cannot also be assured that the material they are seeing – although deemed 'most relevant' by the algorithm behind the search engine – is actually the best and most reliable material for their purposes. Like any fishing net, search engines are prone to collecting plenty of flotsam and jetsam along with the intended catch. Finally, without adequate security precautions, online searches are notoriously blatant ways to collate intelligence, especially when it comes to sites where personal information might appear, such as professional development or social media platforms.

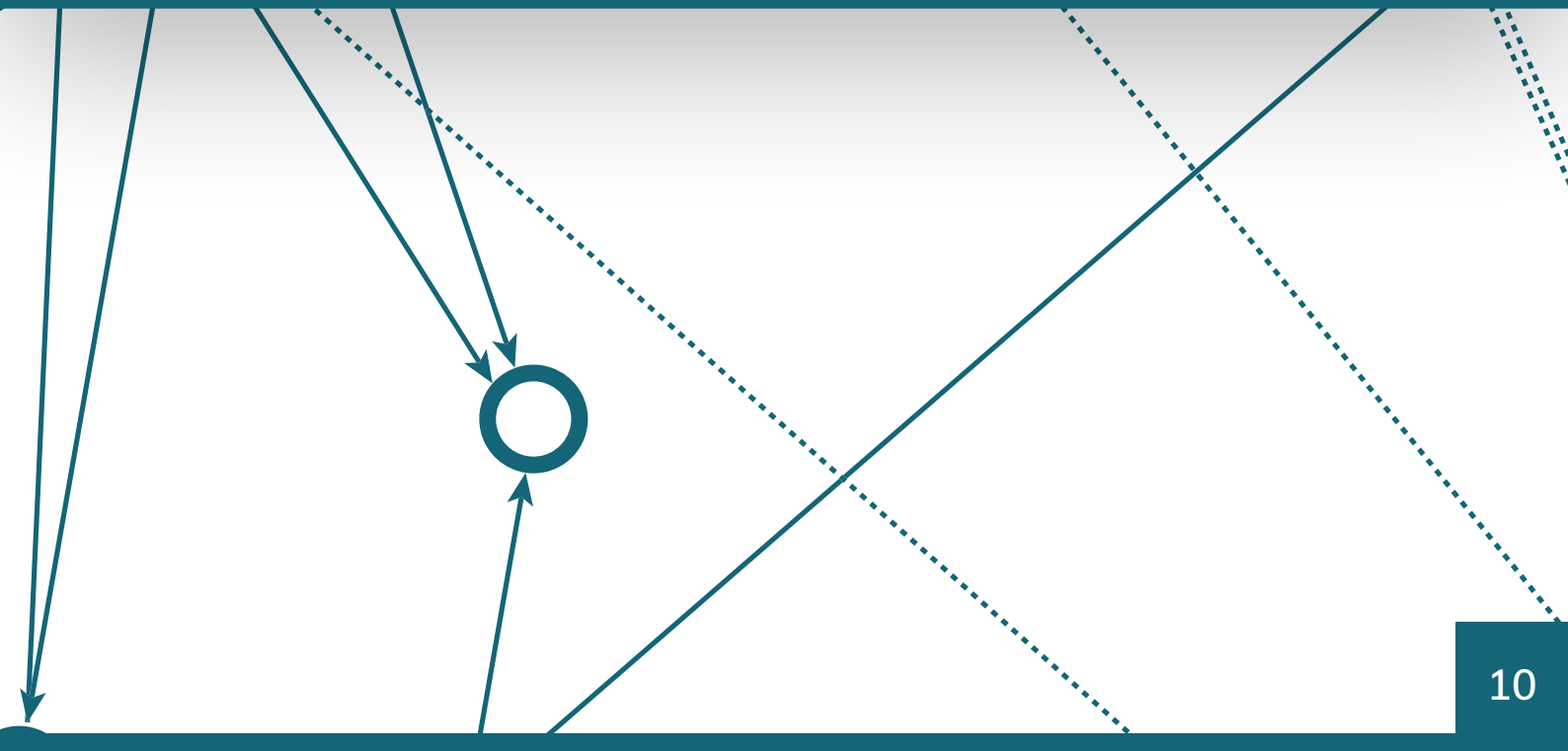
Some financial institutions have learned these lessons and have sought to take a more tailored approach, sourcing information through large market data and adverse media providers. Nonetheless, even these solutions face similar volume and prioritisation problems to the Internet, along with the tendency to be curated in a 'one-size-fits-all' way that stress the number and range of data sources without references to the specific needs of the customer. Even where they offer large amounts of data, such solutions are also limited in scope because they do not provide access to all of the data that might be relevant. Using 'walled gardens' of data exclusively is unlikely to provide the insight that the internet can.



Targeted OSINT Solutions

Luckily, there are better ways for financial institutions to tap into OSINT without being overwhelmed by a tidal wave of irrelevant material. Beyond the internet and more rudimentary vendor solutions, the sector is increasingly seeing a range of dedicated OSINT platforms that have been designed clearly with the needs of the analyst or investigator in mind. The best examples of these are able to tap into the full spectrum of online sources while also delivering carefully curated results which can be easily visualised, prioritised and searched.

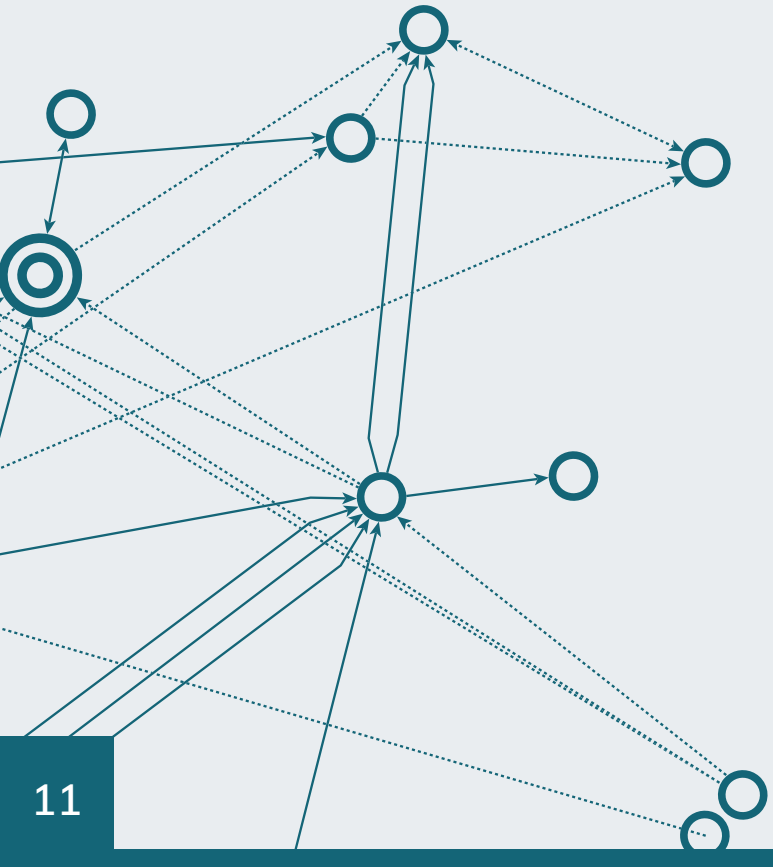
Such best-in-class solutions remove the need to wade through swathes of irrelevant or questionable material, because considerable preliminary curation of available open sources has already been undertaken. This process identifies the best sources available for different types of investigative problems, and brings these sources into a single platform, as well as combining them with feeds from within the financial institution. Applying rich in-built analytic capability, such platforms allow the investigator to both 'trawl' widely, whilst also 'spear-fishing' for the most germane material available. Investigators are thus able to work a case in a fluid but structured way, with full confidence about the credibility of the data sources they are using.



Conclusion

Due to the rapid and continuing growth of publicly available and accessible data, we might very well say that what we now live in is the 'Age of OSINT.' Never has so much beneficial intelligence been potentially directly available to those who need it. And yet, as discussed above, the utility of OSINT is still not fully appreciated in all quarters, including the worlds of compliance and risk management in the financial services sector. There is still a tendency in many firms to look only to their own internal data for answers, or to think of intelligence as the engagement of firms which conduct 'cloak and dagger' style operations. This is a missed opportunity, as the innovations of a select group of leading financial services providers are demonstrating.

Faced with significant financial crime – and regulatory – risks, these firms have found the intelligent deployment of OSINT to be a crucial and cost-effective ingredient in the renewal of their anti-financial crime frameworks. Not only can it improve the functioning and outcomes of core compliance processes as they stand – it can also support the development of more risk-driven and proactive ways of fighting financial crime in the private sector.



As these firms have also found, however, it is not simply enough to embrace the idea of using OSINT; it has to be done with intelligence and care, too. The internet is a highly valuable data source, but reliance on search engines risks overwhelming analysts and investigators with irrelevant or low-quality materials, leading to wasted time, inefficiency and poor outcomes. As an alternative, financial institutions need to look at other available solutions that can allow investigators to harness the huge potential of the internet, in a secure and user-friendly environment. The essential task is to find a partner with the experience and capacity that can deliver the kind of efficient, targeted and outcome-driven approach to using OSINT that financial institutions need.

Collect, analyse and visualise open source data with Videris

Blackdot Solutions makes Videris, a complete online investigations and intelligence platform for professional investigators and analysts.

Contact us to see Videris in action and find out how we can help to take your capabilities to the next level.

Get in Touch