MOODY'S

# BUSINESS ACTIVITY INTELLIGENCE (BIZINT) IN ACTION:

## The power of corporate data footprints to interdict national security threats

March 2025

# Introduction

Law enforcement and intelligence agencies are locked in a chess game with their criminal organization adversaries. This is especially true with foreign nation state-sponsored and terrorist groups. To avoid detection and capture, bad actors rely on staying several moves ahead. For investigators, the enduring challenge is that the game has fundamentally changed – and not in their favor.

Thankfully, investigators can exploit a key weakness. By leveraging publicly available or accessible data, they can follow bad actors who are unwittingly leaving footprints in public records. This is known as business activity intelligence (BizINT). A form of open source intelligence (OSINT), BizINT leverages organic economic and commercial data to provide an "honest broker" lens on indicators of fraud and other wrongdoing: it represents the paper trail left behind when societal norms compel bad actors to participate in professional and revenue-producing activities – or to use recognized instruments and mechanisms for commerce.

Such intelligence's value to investigations is significant yet relatively underplayed. Indeed, business activity footprints can help provide color not only to financial crimes like money laundering, but also to physical crimes with a financial nexus, such as drug trafficking, human smuggling, terrorism, counterfeiting, and more. In this eBook, we explore BizINT's roots, applications, and benefits to the intelligence cycle.

## Sophistication of adversaries breeds complexity

Undoubtedly, the modern adversary has become more sophisticated than in past decades. The most difficult to intercept are criminal networks and adversarial organizations, such as terrorist organizations, racketeering conspiracies and espionage rings. Such groups – typically nation-state or sub-state sponsored – are not only strategic and well-resourced. They operate much in the same way as legitimate organizations, adhering to bureaucracy, setting strategic priorities, and even budgeting. They also typically adopt one of a myriad of command and control models – from centralized structures, to federacies, to a convoluted hive of affiliated actors operating independently of one another.

Yet, no matter how they operate or what chain of command their employees adhere to, it's clear that such organizations are well-versed in the tradecraft of professional investigators and intelligence services. They understand how the research and query process works, along with what's needed to establish more than just a circumstantial picture of wrongdoing.

Only complicating matters is that bad actors can make use of widespread dual-use technologies to obfuscate their nefarious activities and often non-obvious intentions – even misdirecting or surprising investigators. Terrorists, foreign spies, and sophisticated criminals no longer conduct harmful activities on an information delay. Instead, they can near-instantaneously communicate and exchange information – enabling them to stealthily mobilize at lightning speed.

### The emerging complications of combatting nefarious activity

## An introduction to open source intelligence

Against a dynamic threat landscape, investigators have no choice but to adapt. Yet sometimes the oldest methods are among the most effective. First coined in 1941, and as old as the United States' modern national intelligence system, open source intelligence (OSINT) remains a valuable resource.

During the past seven decades, open-source content has expanded beyond media reports to include academic publications, conference content, presentations at trade shows, public speeches, and local data reports. In more recent decades, internet and social media content has fallen into scope, too.

Whether for the purposes of societal transparency or commoditized as a product for sale, public records track the day-to-day activities of companies, individuals, and special interest groups. They can provide a myriad of frequently-updated datapoints that cover various aspects of a person's or organization's identity, status, behavior, skills or expertise. Typically, public records add color on two of the "five 'W' questions" (who, what, where, when, why). These are most often (though not exclusively) the "who" and "what they are doing."

BizINT, meanwhile, is a form of OSINT – and, arguably, the most powerful. Where other OSINT types might speak to two of the "five 'W' questions", BizINT can address the who, what, where and when – and, in some circumstances, even the "how". Crucially, its detail is sufficient enough for investigators to conduct pattern and trend analysis.

Much like an orchestra, BizINT is distinctive from other types of OSINT (such as human intelligence, or measurement and signature intelligence). Yet, when layered on top of one another, the result is greater than the sum of its parts. Let's take signal intelligence (SIGINT), for example, which entails the interception of electronic signals and communications. Any intercepted signals could be cross-referenced against business activity data to ascertain the "why" and "how" business registration, transaction, or event and what it means relevant to the broader common operating picture of the entire threat being examined. Likewise, imagine taking commercial real estate (CRE) data and correlating it with cell tower pings gleaned from phone records acquired through a warrant. This could confirm that phone activity associated with a particular individual is now also affiliated with a building also known to be owned or occupied by that same person.

### What constitutes BizINT?

BizINT, therefore, makes use of the data footprints from bad actors' day-to-day activities and engagements with legitimate systems, which every individual or organization – reluctantly or unwittingly – leaves behind.

These footprints can tell a colorful story: they can be compared to the typical participant as a baseline, or provide intelligence on company size, revenues earned. Investigators can use these footprints to discover or confirm an identity, and connected persons of interest – as well as how actors may intend to commit crime or pose a threat (their means and methods).

In the game of cat-and-mouse, savvy criminals are already aware of the footprints they leave. Indeed, by thinking how their suitors will think, criminals can build an understanding of what BizINT trails they're leaving for investigators to find. Even savvier ones can even throw an investigation off course by leaving erroneous trails. Investigators can regain parity in the chase, however, when a criminal unwittingly leaves an accurate footprint that cannot lead to misdirection.

Databases that simply record business activities and transactions, without predefined criteria for identifying illicit behavior, provide investigators with an impartial source of information. This allows them to objectively identify events that meet the threshold for nefarious activity, free from biases or preconceptions about what to look for. When proactively searching for fraud and other wrongdoing, accidental selection bias may occur. This could, in turn, skew the accuracy of eventual key judgments an investigator needs to make.

## Four critical ways business activity footprints offer color and close knowledge gaps

Business activity footprints provide critical insights across four areas. The first is **conduct contextualization**, where legitimate business activities – when analyzed in the context of information from other sources – support the hypothesis that a person or entity is involved in a broader nefarious agenda.

For example, if recently-updated public records indicate that a known Russian oligarch is now the beneficial owner of a Russia-based company that owns a Sweden-based company, which ultimately owns a U.S. company of interest, this activity would fall under the method called "obfuscation by structuring". This allows a casual onlooker to assume there is no association with the oligarch due to several degrees of separation.

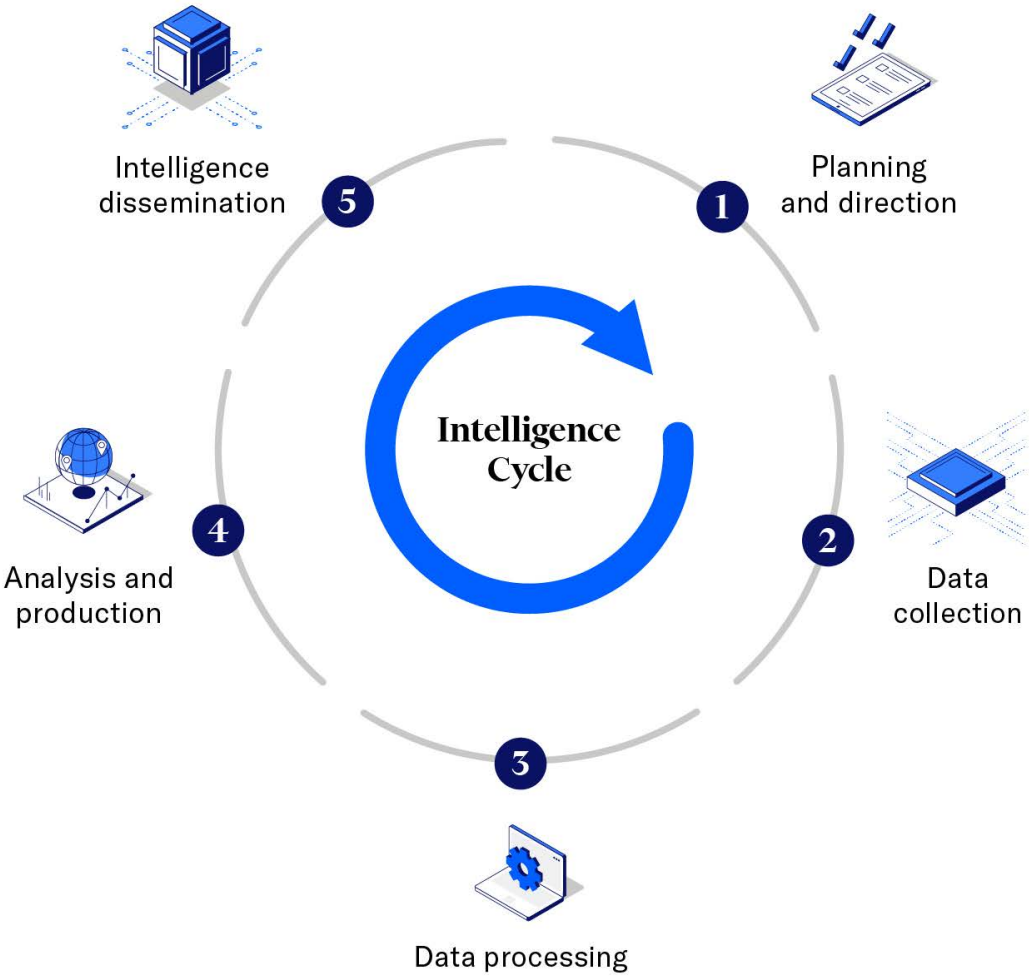
**Position contextualization** confirms a person or entity's permanent operations base or their locations during a certain period. Geolocation can be achieved through ownership of commercial and residential properties, employment history at multiple firms in one country or geographical region, and public or commuting trend transportation data. Similarly robust information can help analysts assemble heat maps, and track physical migration, the route of goods, or the frequency of repeat travel.

**Access contextualization** characterizes how people and entities have the means and opportunity to associate with nefarious activities with some degree of probability. For instance, a known drug trafficker revealed to be an executive-level employee of a chemical precursor manufacturer not only has access to large quantities of a chemical ingredient to produce a drug of concern – but their leadership role presents clear command and control over the chemicals, distribution partners, and routes in order to ease the drugs' movement through mostly-legitimate transportation channels.

Lastly, **activeness contextualization** describes the pervasiveness of participation in business activity directly related to facilitating nefarious or illegal activities under investigation. While a bad actor can establish plausible deniability of a single incident that associates them with wrongdoing, a large number of repeated transactions, transactions occurring over a long period clearly presents a situation that cannot be explained as coincidental. In turn, this can provide persuasive information for justifying subpoenas and warrants.

Business activities can inspire questions around collection requirements that could revive an investigation when investigators are stumped from reviewing other sources – or when they are unsure where to even begin. In other cases, investigators have formulated questions to start asking but consult business activity data to confirm if they are asking the right questions, confirm pre-existing assumptions or actually lead to refining questions to focus on the right details.

# The intelligence cycle's five steps




So, where does BizINT feature in the traditional intelligence cycle? After the data collection phase, BizINT can be combined with a variety of disparate or unstructured information to make better key judgments. For instance, if the investigation uses social media content as a source, BizINT can provide a more objective view for corroborating any claims – especially since social media content relies on self-disclosure, which can be inaccurate or intentionally misleading.

BizINT also features prominently again during the production and analysis stage as an enhancement mechanism. BizINT further refines finished intelligence, and offers a view on its reliability. Once individual datapoints in business activity records are corroborated with other factoids in the same repository, investigators can apply inductive and deductive inferencing, and build an overall common operating picture.

As with all forms of intelligence, actionability is paramount. To this end, most professional intelligence services employ a "So What Matrix", which helps investigators identify a desired outcome from collecting a piece of raw information – and its relevance to enhancing the knowledge baseline about a specific target, risk, threat, or uncertain issue. At minimum, investigators expect that raw information will have enough value to create a lead or line of inquiry.

## How "So What Matrixes" can propel an investigation

| Possible So What Matrix outcomes | Why is it important? |
|---|---|
| **New entity discovery** | Companies and individuals who are listed as beneficial owners, officers, or executives |
| **New relationship discovery** | First- and second-order connections to an organization or another person |
| **Close knowledge/factoid detail gaps** | Timeframe/dates of involvement with an entity, what countries the subject/target has business presence |
| **Confirm facts, events, characteristics gleaned from other sources** | Verify or refute key assumptions |
| **Understand qualitative nature of what business activities target/subject involved in and how they might be doing it** | Industry, business size, business type, activity/dormancy along with business structures (holding companies, subsidiaries) and merger and acquisition (M&A) activity |
| **Order of magnitude** | Frequency of transaction, number of businesses owned in a country, organizations with like-name variations |
| **Data attributes that violate expected values or range of values** | Anything quantifiable about an entity or its activities |
| **Obfuscation through intentional backstopping to make public footprint less obvious** | Normalization of data attributes controllable by the target/subject in a way that will make it difficult for an analyst to measure the certainty of anomaly or adverse nature |
| **Delta/evolution in data attribute** | Status, dates, business name changes, board member movements, number of associations, etc. |
| **Adverse alerts** | Sanction and politically-exposed person (PEP) status, regulatory/lawsuit filing disclosures, judgment, liens, bankruptcies, failure to make timely filings or non-compliance with registries. |

## Which bad actor agendas can BizINT uncover and interdict?

BizINT can address four types of bad actor behaviors, known as the "four Cs": control; concealment; circumvent; and conduit.

These four behaviors are crime- and threat-agnostic. Rather, a safe assumption is if one can successfully uncover nefarious behaviors in their early stages, adverse outcomes can be mitigated before the actor can conceive a specific attack, event, or point of penultimate victimization.

## Delving into the four Cs

| Behavior | Description | Risk profile domains | Example methods |
|---|---|---|---|
| Control | The desire by a person or organization to have direct command or tasking authority over business operations to achieve an envisioned impact on a counterparty or counterparties participating in the same or a related commercial environment. | Economic espionage; synthetic drug manufacturing; organized crime; counterfeiting; conspiracy; tax evasion; real estate/property management | Hostile mergers or takeovers, strategic duress; bad actors access non-public information by inserting themselves in a position of authority. |
| Concealment | Active attempt to hide, deny, misrepresent, or disassociate a person or entity's identity, status, bona fides, mission, and conduct in order to avoid detection and/or punishment for involvement with some type of illicit or outlawed activity. | Economic espionage; identity fraud; organized crime; terrorism, conspiracy; money laundering; human trafficking; legalized marijuana | Synthetic identity fraud |
| Circumvent | Active attempt to evade or avoid rules, regulations, laws, accepted industry practices or other requirements that guide the ethical and appropriate conduct of everyday professional activities; concerted acts to outwit a counterparty in the broader market through surreptitious means. | Economic espionage; cybercrime; money laundering; counterfeiting, weapons trafficking, prostitution; extortion; document fraud | Evading sanctions using proxies, opaque state-owned enterprises, family members and associates, or the use of enablers e.g. lawyers and accountants |
| Conduit | Use of completely legal means, vehicles, channels or mechanisms to facilitate an ultimate illicit act or create an adverse outcome against a specific counterparty or range of counterparties in the market/ society. | Economic espionage; loan sharking; public corruption/bribery; conspiracy; identity theft; mail and wire fraud; sanctioned foreign investment | Shell companies |

## Looking ahead: the role of platform software and the advent generative artificial intelligence (GenAI)

The challenges law enforcement and intelligence agencies face in combating criminal activities are only compounding in an increasingly complex landscape. Nonetheless, BizINT can uncover rich and actionable information that closes the gap, providing investigators the necessary context to effectively identify and track criminal activities.

For the past two decades, intelligence automation software has centered on network graphs, which allow analysts to view the target criminal network in a holistic and visual way. A key feature of automated network graphs is the ability to change the central node at a click of a button, which is critical for analysts to view the network from a new perspective. That said, network graphs have undergone few advancements during this period, with the exception of systems that can respond to queries about a set of pre-loaded data.

As such, investigators are now looking for software platforms that can house heatmaps on which investigators can plot the locations of persons of interest, and visualize key information, such as their possible transportation routes to one another, the density of business activity in the area, and much more. Other features may include timelines that can show events sequentially, as well as key milestones, and activity gaps, etc. in order to detect patterns, and build a holistic operational picture.

Another critical tool are decision trees, which can be used to map out alternative scenarios based on various dependencies or drivers. This is particularly important for If-Then Conditional Analysis, where investigators determine what would have to occur before a particular event meets the threshold of a threat or adverse event.

Of course, further technological assistance is always welcome. With this in mind, one emerging trend that law enforcement agencies must pay close attention to is the advent of generative artificial intelligence (GenAI), which offers a raft of exciting possibilities.

The first is in data analysis. By analyzing vast amounts of data from various sources, GenAI interfaces can enhance the analysis of business activities, as well as predict and identify criminal patterns. One of its main advantages is identifying non-obvious observations, uncovering new gaps, revealing interesting correlations and causations, and assigning probabilities to predictions or forecasts. It can also be used to generate comprehensive reports that highlight anomalies and potential threats – as well as build scenario models that could help agencies to anticipate and counteract criminal strategies proactively.

Additionally, GenAI's next-level natural language processing capabilities can assist in translating and interpreting data across different languages and formats, broadening the scope of intelligence gathering. These advancements enable law enforcement agencies to stay a step ahead when adversaries engage in cat-and-mouse, making it harder for criminals to hide and operate undetected.

But the possibilities do not end there. In the coming years, GenAI is expected to significantly augment the value of color analysis – particularly in scenarios where attention to detail is crucial for deriving actionable insights. Three key application types that will likely be exploited are GenAI-powered Q&A chat interfaces, data interrogators, and inference engines.

For instance, in qualitative analysis, a Q&A chatbot may help investigators identify unknowns and knowns, as well as trends and changes over a given time horizon. In dynamic triage situations, AI can distill asymmetric data point combinations and enable querying from visualizations rather than just the underlying database. An inference engine, meanwhile, applies logical rules to a knowledge base in order to facilitate various forms of reasoning – such as deduction, induction, and abduction – to help analyze and interpret complex datasets in a fraction of the time.

Of course, the race against criminals is ever-going. In our view, BizINT is among the best weapons in the investigator's arsenal. And, the technological evolution that is already underway promises to further augment the capabilities that law enforcement agencies have at their disposal in the enduring battle against sophisticated criminal networks.

MOODY'S

For more information, please visit:
www.moodys.com/publicsector

March 2025