



Use of Intelligence in Financial Cybercrime Investigations

March 2023

Stopping financial crimes is a multifaceted challenge, and the increase in cyber threats has made this significantly more complicated. According to PwC, external economic crimes cost the firms they surveyed \$42 billion annually.¹ As investigators quickly navigate change, bad actors look to exploit any widening gaps in investigation capabilities. As reported by the World Economic Forum, we are gradually seeing the rise of risk management rather than compliance-run cybercrime strategies to combat these threats.²

Do the public and private sectors need a more proactive and focused approach to cybercrime risks and threats, especially concerning investigation intelligence?

Generating intelligence involves collecting information on cybercrime from a wide range of private, public and open sources and then processing and analysing that information. The objective is to enhance and grow intelligence, which will help the investigator fight cybercrime as effectively as possible.

Investigators and Intelligence

The cybercrime investigator is at the forefront of the fight against financial crimes, undertaking an array of intelligence collection and investigative tasks. This involves using multiple analytical platforms, investigative tools, open-source intelligence, and other tools, which are constantly evolving. Thus, the techniques and tools keep changing. It happens often, investigators' desks jumbled with paperwork, computers with multiple standalone applications and separate computer screens to keep up with the volume of wrongdoing.

Cybercrime investigations continue to be hindered by a fragmented approach. Numerous digital devices have proprietary operating systems and software that require specialised forensic tools to identify, collect, and preserve digital evidence. The time taken to investigate everything can seriously hamper or delay the identification of crucial evidence in an investigation.

Much of this approach is driven by the low quality and ungraded intelligence that investigators receive. Poor source material and inadequate analytical platforms can, in turn, generate a *'throughput mentality'* amongst investigators, where the focus is less on the quality of the investigation and more on ensuring that volume-based targets have been met.

Intelligence grading, however, is a fundamental step in the intelligence process by investigators and others. Why? So, anyone reading it can have the confidence to depend on it. Once gathered, intelligence should go through a grading process where a handling code is attached to the content as part of an initial risk assessment process. Grading intelligence allows for a quick and accessible expression of this intelligence source risk assessment and sanitisation to protect that source. Based on this grading, an investigator can begin prioritising devices to review.

Cybercrime Investigations and Intelligence

Financial cybercrime investigations happen regularly within financial institutions ("FIs"). Their quality can vary widely in many instances because FIs often do not work with optimal analytical and forensic tools or intelligence sources. Many FIs still use standard word processing and spreadsheet applications to collate, store, and analyse customer behaviour or first-generation analytical platforms to identify vital transactional relationships. Investigators must also work through various disconnected internal and external sources to collate material for their investigation.

Notes

[1] <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>

[2] <https://www.weforum.org/agenda/2020/02/cyber-risk-should-take-centre-stage-in-financial-services/>



Cybercrime Investigations and Intelligence (*continued*)

The proliferation of separate data sources and intelligence streams can decelerate the investigation process, creating voids that allow mistakes and potentially missed connections that will undermine the value of the final assessment produced by the investigator. This ‘multiple system’ approach makes the investigation process more challenging to record, manage, and ultimately audit.

Despite efforts by regulators and authorities to continuously develop their strategies to fight financial cybercrime, bad actors continue to adapt, leading to more sophisticated threats and attacks in all areas of financial cybercrime. There are also significant challenges with ensuring that investigators get the right kind of contextual intelligence delivered in a way designed to support robust outcomes. Some of the problems an investigator may face include:

- **Quantity of intelligence** – this is a matter of either feast or famine, especially concerning the open source intelligence (“OSINT”) framework.³
- **Quality of intelligence** – the provenance and reliability of material are often hard to assess and lead to extended and fruitless efforts to corroborate information.
- **Consistency of intelligence** – for example, open-source searches on the internet will often produce results that vary depending on location, past user history, or what online vendors might be seeking to sell. The internet is not designed to help investigators find information.
- **Security of investigations** – some investigations can leave potentially glaring online footprints on more sensitive sites such as social media platforms.
- **Use of digital evidence** – the primary goal of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence, and present the findings.

Evolution of Investigations

Experienced and well-trained investigators can help mitigate some of these problems, but even the best investigator must be equipped with the correct data and tools. A significant development is the advent of ‘intelligent automation’, which combines artificial intelligence and robotic process automation to put investigators at the centre of seamless and carefully curated intelligence environments.

These environments make the collation, analysis, and assessment of material as frictionless as possible by:

- Producing an **all-around view** – rather than following numerous lines of intelligence on various platforms, investigators can work through a primary platform that brings together the right kind of graded intelligence – internal and external – in a single space in the shortest time possible.
- Refining the **intelligence deluge** – instead of chasing down untold disparate sources from scratch, graded and improved intelligence allows an investigator to start with a solid set of foundation stones.
- Developing a **structured approach** – investigations can rapidly become unstructured as they move across different evidential sources. Having a structured dashboard will facilitate a more systematic approach.
- In this modern age of technology, **digital evidence** is an integral part of an entire intelligence and investigation process. It helps investigators capture critical intelligence and evidence from computer systems and networks. Digital intelligence and evidence are growing exponentially and must be managed appropriately throughout an investigation.

The decisions made by financial investigators within FIs are incredibly significant and can influence management decisions or the future of a customer relationship. If genuinely suspicious activity is missed due to poor investigative practices, poorly equipped analytical platforms, or inefficient use of intelligence, a crime that might otherwise have been detected and disrupted will be allowed to proceed. Having the best investigative tools to hand enables organisations to make these kinds of risk-based decisions confidently. At the same time, similar failings could lead to an innocent person being treated as a subject of concern, raising issues of fairness and having implications for financial inclusion. Whether the investigator gets it right or wrong will significantly affect how well an FI tackles financial crime, keeps its reputation intact, reduces monetary loss, and protects its customers.

Note

[3] <https://osintframework.com/>



Way Forward

Investigator-led approaches have better success against high-profile risks using improved and integrated intelligence settings within the intelligent automation process. Their deployment within the financial services sector for cybercrimes is already beginning to show fruit, primarily when allied with closer cooperation across private and public sectors in sharing risk information. As financial cybercrime practitioners focus increasingly on delivering results, it seems evident that empowering the investigator with the right tools to automate, collate, and grade intelligence will significantly aid the quality and efficiency of investigations.



Contacts



Darren Mullins

Partner

darren.mullins@accuracy.com
+971 56 682 5681



Paul Wright

Senior Adviser

paul.wright@accuracy.com
+971 522 449429



Arthur Couvreur

Director

arthur.couvreur@accuracy.com
+33 6 66 69 65 15



Steve Molloy

Director

steve.molloy@accuracy.com
+39 334 10 49 578

Accuracy partners and professionals are available to discuss your needs and design an appropriate solution with the relevant experts.