The Mindset of Financial Investigations, an "Out of the Box" Approach

By : Dr. Paul G. Morcos *

Banks and Financial Institutions, as part of their compliance duties, perform investigations of financial transactions that are suspected to involve money laundering, fraud, and corruption, as well as, other categories of financial crimes.

Therefore, they invest in human resources and management information systems to assist in the identification of unusual transactions and suspected criminal activity for the purpose of protecting the community and the soundness of the institutions.

FATF Definition (1)

The Financial Action Task Force (FATF) defines the term financial investigation as an inquiry into the financial affairs related to criminal conduct. The major goal of a financial investigation is to identify and document the movement of money during the course of criminal activity. The link between the origins of the money, beneficiaries, when the money is received and where it is stored or deposited can provide information about and proof of criminal activity.

Overview

In the current practice, financial investigators aim at identifying suspicious conduct or activity by collecting and analyzing all available information. They are constantly eager to recognize trails or indicia that can be followed and traced to identify any potential evidence of financial crime.

An Investigative Mindset

Most commonly, the AML compliance investigation follows a straight-forward set of procedures initiated by reviewing the transactions; investigating the beneficial owners and associated parties; and developing an assessment of alerted transactions.

In the most recent years, new practices and techniques started to rise, thus, shifting the investigation process to a new mindset. Financial Crime Investigators are setting new tones for their investigations. They do not only seek to determine the nature of account activity or analyze the reports generated by their monitoring systems, but also they have started collecting information from various sources of alerting systems and transactions; identifying patterns of complex behaviors – mainly used to layer the criminal proceeds; and analyzing those patterns and alerts.

The final decision of an AML investigation is frequently seen in the filing of a Suspicious Transaction Report (STR) of a certain type of transaction or a group of individuals or entities.

Investigative Techniques

Reviewing customer information and transactions is an essential process of an effective compliance-monitoring program. Criminals constantly try to take advantage of the banking products and services which are evolving due to the technology progress. In parallel, banks and financial institutions are obliged to review and enhance their investigative techniques towards a combined

* *(Professor, Legal consultant for a number of Lebanese banks for compliance, owner of JUSTICIA lawfirm: www.justiciabc.com)*

connected into workflows, with both manual and automated approval steps. This structure allows organizations to more speedily and consistently follow response policies and procedures, yet incorporate human and dynamic decision making.

Summary

An effective defense against advanced threats hinges not only on being able to detect pernicious intruders, but doing so in time to prevent significant damage to business operations and assets. This negative impact is the key variable in the risk equation: Risk = Threat x Vulnerability x Impact. By the time forensic analysts comb through mountains of security data looking for indicators of compromise (IoCs), their organizations may have already incurred losses. This report aggregates front-line experience to present the key steps organizations can take to harden their infrastructure, improve their responsiveness, and actively disrupt targeted attacks by paying attention IoAs. It includes ways to learn from each interaction, enforce consistency, connect the smoke signals of an attack, and create an actionable, real-time picture of dynamic events.

A real-time SIEM is a significant enabler, since continuous monitoring and advanced analytics allow security managers to identify IoAs quickly and accurately.

Integration can even catalyze instant action to contain and remediate the attack.

But the reality is that technology is not always the problem. Many of the countertactics mentioned here can be implemented with existing countermeasures and an integrated incident response program.

The information most helpful to success can be recognized and mitigated today with adequate people and process and with technology organizations many have already deployed. The call to action for risk and threat managers is to focus on time management: improving their ability to detect, respond to, and learn from events as they unfold—thinking and acting within a timeline expressed in minutes. This mature approach to proactive incident management as part of an overall risk management strategy offers the most agile and effective protection against targeted attacks.