Deloitte.

Digital Forensic Readiness
The time is now

March 2022

MAKING AN IMPACT THAT MATTERS since 1845

The increasing reliance on technology for delivering value brings with it the inherent risk of Cybercrime.

In the digital era, it has become imperative for responsible organizations to maximize the use of technology to detect and respond to fraud they may be exposed to.

To achieve this, organizations must take proactive steps to ensure they have adequate people, processes and technology in place to perform digital forensic investigations.

The increased reliance on technology by organizations, especially financial institutions for both internal operations and customer service delivery has given rise to a new source of risk. The risk that technology could be used for financial misconduct is not only present but also rising. Additionally, regulators are increasingly mandating banks to ensure they have timely access to cyber forensic expertise. CBN in its Risk based Cybersecurity Framework Exposure draft of 2021 advised banks to set up a forensic lab or sign up to external cyber threat intelligence services to manage their digital fraud risk.

According to Nigeria Inter-Bank Settlement Systems, in 2020, the Nigerian Financial Services industry lost more than NGN5 billion to fraud.

Digital Forensic readiness is the attainment of an acceptable level of capability to collect, preserve, protect and analyze digital evidence so that it can be used as part of an investigation. A digital forensic framework should contain the following:

- Well defined investigation strategy which includes an investigative methodology that aligns with the need and goals of the organization.
- Personnel with digital forensic expertise such as certifica tions, industry experience and membership to global digital forensic associations.
- Access to cutting-edge technology with support for current cybercrime landscape.

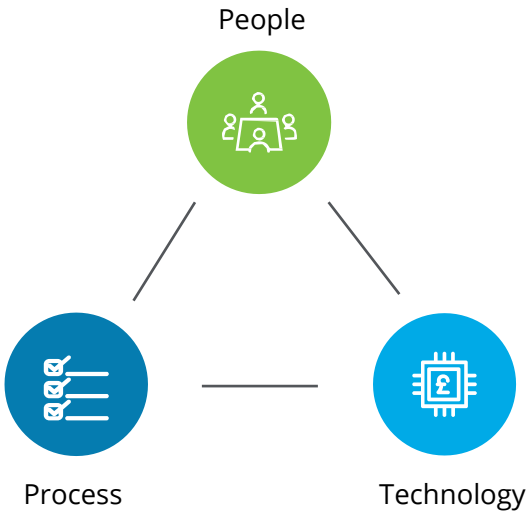
Organizations should also have an anti-fraud policy that incorporates the risk of fraud using technology and outlines the procedures for responding. A clearly defined strategy ensures resources are properly allocated and the investigation methodology is aligned to the needs of the company. Additionally, every investigative procedure should be well documented and authenticated to ensure the admissibility of evidence in court.

Digital forensic investigations require specialized skillset and in-depth knowledge on the inner workings of data, data sources, data analytics, evidence handling and document review. Fraudsters in this space are known for their versatility and always changing tactics used to evade detection. Hence, the need for experienced digital forensic investigators cannot be overemphasized. It is also beneficial for investigators to be part of communities where they can share resources and experience about the ever-changing cybercrime landscape.

Having the right tools can be the difference between identifying a smoking gun and losing millions in fraudulent transactions. Due to the nature of digital investigations, tools are specialized to particular functions in the investigation lifecycle including data collection, analytics or document review. Hence, the development of digital forensic capacity can be a very capital-intensive project for most organizations. Availability of the appropriate tools can also impact the turn around time for investigative cases.

Appropriate synergy between people, processes and technology is necessary to effectively respond to issues of misconduct by both internal and external parties.

The Triad of Digital Forensic Readiness



Once an organization has made the decision to develop its digital forensic capability, it will also need to decide the deployment model that suits its needs and incorporate this model into its strategy. To determine the best model for an organization, considerations need to be made concerning cost, expertise, cybercrime landscape and existing regulations.

Digital Forensic Laboratory Deployment Models

In-house Lab

An organization may decide to develop the capability to perform every step of a digital investigation in-house as part of its fraud risk response strategy. This approach allows for a quick response time as the team is already well versed on the policies and procedures of the company.
However, this approach can be very cost intensive as tools will need to be acquired and license subscriptions will need to be paid even when the tools are not fully in use.

Retainership

An organization may enter an arrangement with a professional third party that allows it to leverage tools and expertise in performing digital forensic investigations based on the terms of the agreement.
The cost of acquisition and maintenance of the tools is transferred to the third party & there is little to no on-boarding process, thereby allowing for a quicker reaction time. This approach also allows the company to lower cost by negotiating discounts.

On-Demand

This approach allows the organization to access digital forensic services when the need arises.
Every investigation project will involve contracting a third-party investigations team.
In this approach, the organization only pays for the services it utiilizes during an investigation.
Delays may arise due to the on-boarding and off-boarding of investigators.

The time to incorporate a digital forensic investigative capacity into your fraud response strategy is now. Every second counts when an incident occurs, and it is imperative that your organization is ready.

Contacts

Beulah Adeoye
Forensic Leader
Deloitte West Africa
badeoye@deloitte.com.ng
+23419041929

Abayomi Aina
Manager Forensic,
Deloitte West Africa
abaina@deloitte.com.ng
+23419042220

Babajide Okunlola
Manager, Forensic,
Deloitte West Africa
bokunlola@deloitte.com.ng
+23419041881

References:

Cybercrime in Nigeria demands public-private action (2020).
Available [Online]:
https://issafrica.org/iss-today/cybercrime-in-nigeria-de- mands-public-private-action#:~:text=In%202018%2C%20commercial%20banks%20in,customers%20and%20depositors%20lost%20N1.

Exposure Draft of the Risk-based Cybersecurity framework and guidelines for other financial institutions(2021), Avaiilable [Online]:
https://www.cbn.gov.ng/out/2021/ofisd/expo sure%20draft%20of%20the%20risk-based%20cyber-security%20framework_august%202021%20pdf.pdf

Fraud in the Nigerian Financial Services
https://nibss-plc.com.ng/media/PDFs/post/NIBSS%20Insights%20Fraud.pdf