Deloitte.

Cyber Risk and Financial Crime – The connected defense

Banche e Sicurezza 2022

Milan, 19th May 2022

The combination of the disruption caused by the pandemic advent, as well as the evolution of cyber threats, have led to a continuous increase in risks to businesses stressing the need to take cyber and financial crime defenses to the next level in the global fight against organized crime

Financial institutions clearly need to embrace advanced technologies such as analytics and artificial intelligence to improve threat visibility and detect fraud effectively, but they also need to have a clear and coordinated strategy to share information, data, and technologies, both internally and externally.

Connect more, to see more, to act better.

Challenges of the new banking landscape

Banks are struggling to keep up wit a rapidly evolving threat landscape

THREAT LANDSCAPE & REGULATION ENFORCEMENT

In recent years, in response to the evolving threat scenario, there has been a **strong proliferation of regulations** that have pushed the FSI market toward a gradual strengthening of organizational and **internal control safeguards**

The regulator is trying to run for cover knowing that the threat landscape is now evolving, **addressing all relevant aspects in countering financial crime**, regulating the management of **payment processes and products** (PSD2 evolution), strengthening **operational resilience** (DORA) and emphasizing **critical infrastructure protection** (NIS2)

CRIMINALS BEYOND BORDERS

Criminal organisations **do not recognise geographical borders** or institutional boundaries

They **operate without recognising any form of segmentation between cyber, fraud and money laundering**. They operate seamlessly, supported by a modern underground market of readily-available software and services

In comparison, **organisations continue to operate in siloes** with separate departments responsible for cyber, AML and fraud, reporting **into different management layers**, each with individual business priorities and goals

DATA SEGMENTATION

Today's approach to data analytics is challenged by the **sophistication of organised criminal groups**

The siloed approach means important data and indicators of compromise are not shared across business units, preventing comprehensive analysis of new complex threats, leaving criminal groups to **undertake illegal activities across multiple parts** of the organisation without being caught

Defences are primarily focused on confirming false positives rather than detection and prevention

The rising impact from cyber and financial crime – some examples

Siloed capabilities and disconnected data inhibit prevention of cyber and financial crime

⚠ EVOLVING THREATS

- Cyber and financial criminals don't distinguish between cyber, fraud and AML
- Criminals run sophisticated operations, with fast innovation and agility

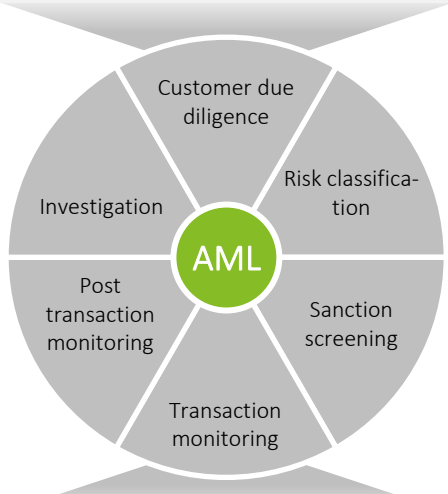
⚠ SILOED CAPABILITIES

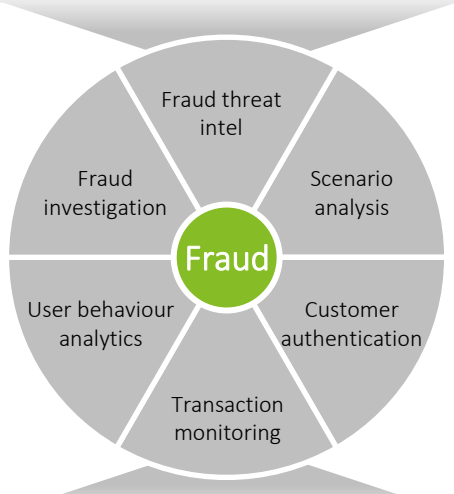
- Reliance on point solutions and manual effort
- Scarce expertise distributed across domains to tackle similar problems in isolation
- Compliance-focused with static rules that are easy to understand

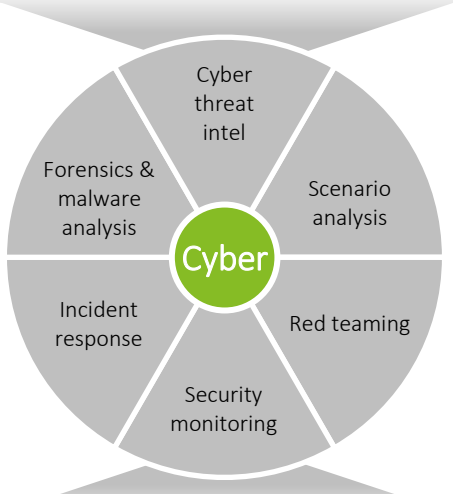
⚠ DISCONNECTED DATA

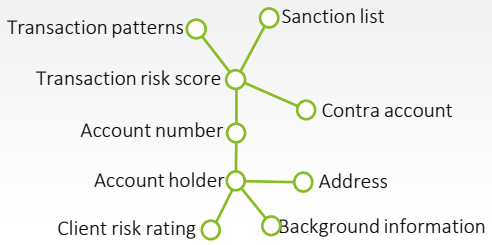
- Separated data streams only cover narrow sections of the attack chain with disconnected data points

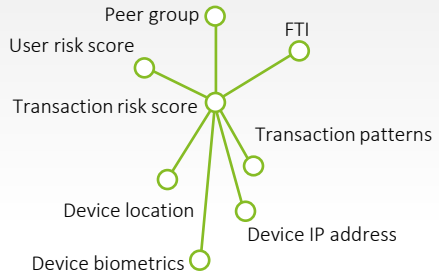
Compromised data used to create mule accounts	Synthetic identities to create fake accounts and steal money	Large scale money theft by APT

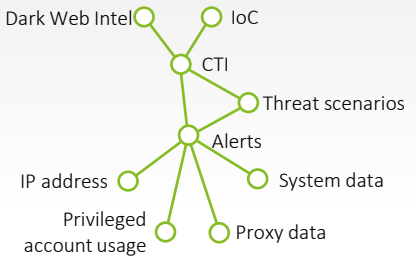












Our Vision: connect more, to see more, to act better

An overarching data and capability model for more effective detection and response

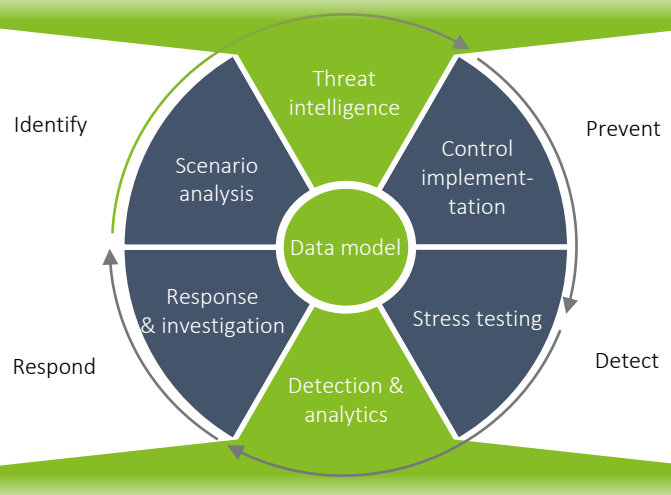
✓ Cross-domain Threat Intel

- Correlate **cross-domain cyber and financial crime intelligence**, instead of focusing on individual items of intelligence within each domain

Compromised data used to create mule accounts | **Synthetic identities to create fake accounts and steal money** | **Large scale money theft by APT**

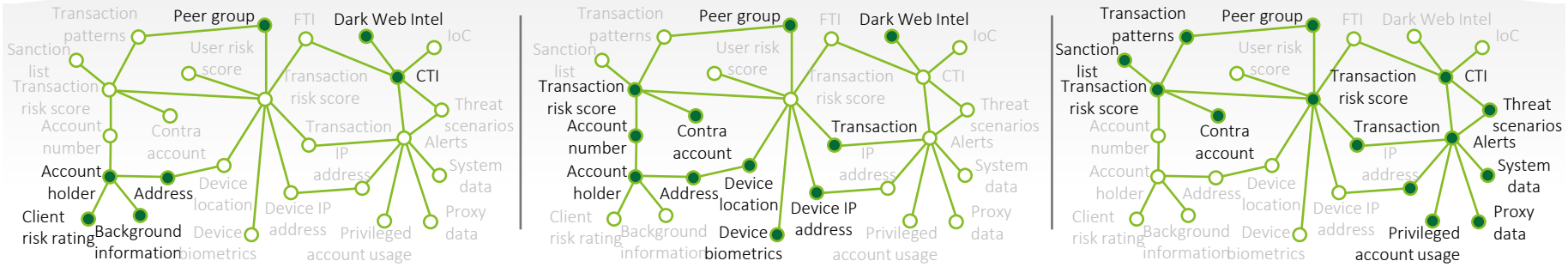
✓ Unified Capability Model

- Scenario analysis to identify and prioritise all cyber and financial crime threat scenarios with a uniform approach
- Control implementation aligned across AML, cyber and fraud to better prevent, detect and respond to threats
- Integral stress testing to validate control effectiveness and drive continuous improvement
- Integrated Detection, Response & Investigation team as a central nerve centre to connect more, see more and act better



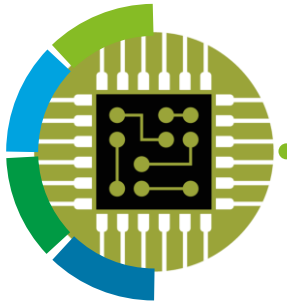
✓ Unified Data & Analytics

- Develop an overarching data structure to collect, classify and correlate data across AML, cyber and fraud



Deloitte's CyFi framework

Breaking down siloes to take Cyber and Financial Crime defences to the next level against organised crime



Embracing new technology and harmonised data…

- Consolidated data and **harmonised technology** improve **efficiency** and **effectiveness** of **detection** and **response capability**, allowing you to **focus efforts** where they truly matter

…to enable end-to-end visibility and response capability…

- **Detection** and **prevention capabilities**, **data**, knowledge, **expertise**, and **budget** are spread across organisational **siloes**, **inhibiting** the **necessary collaboration** and harmonisation of controls across **cyber, fraud, and AML domains**
- **Deloitte's Fusion data model** offers a **comprehensive approach** to combatting cyber-financial crime

…and facilitate more effective collaboration, within and between institutions

- **Cyber and Financial Crime initiative (CyFi)** proposes **breaking down barriers internally** and **between other institutions** to **improve visibility** on cyber and financial crime
- With **complete visibility** across all **data**, you can see **the bigger picture** and **act with greater certainty and efficacy**, reducing false positives and reinforcing regulator and customer confidence

Deloitte's CyFi framework

Our vision focuses on enabling six core components to success

Fused intelligence

Fused cyber and financial crime intelligence to **focus on priority and realistic threat lead scenarios**

Joint response and investigation

Increase the effectiveness of **cyber and financial crime incident response** with **multi-disciplinary expert** investigation teams

Integrated detection

Leverage integrated technology platforms to enable the detection of threats and attacks more **holistically**

Harmonised operations

Harmonise **cyber, fraud, and AML** operations into a **single 'joint' operating model**

Consolidated capabilities and controls

Consolidate **key proactive** and pre-emptive **controls** into a **comprehensive cyber** and **financial crime capability** model and control framework

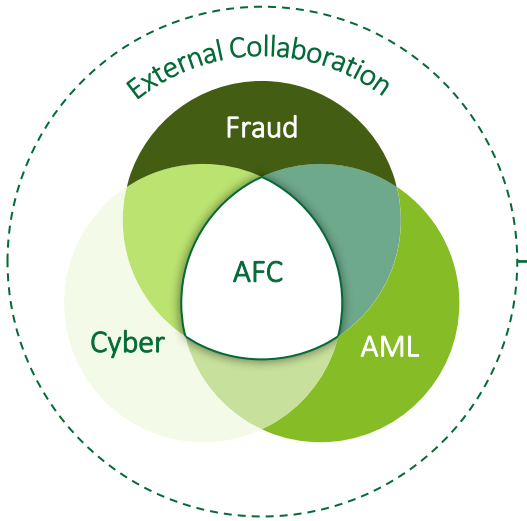
Data science and insights

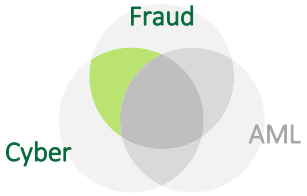
Leveraging a single unifying model to source appropriate **data** from across these risk domains and **enable advanced analytics** to achieve **real-time correlation and insight**

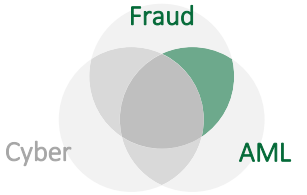
Possible applications of the framework

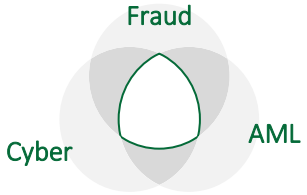
Combining internal synergies and external collaborations to strengthen capacity to address priority risks

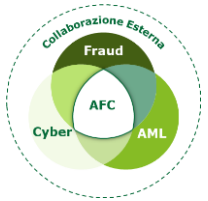
Level of synergy











INTERNAL SYNERGIES

FRAUD – CYBER SYNERGIES

Synergies between the Fraud and Cyber world to anticipate fraud phenomena perpetrated through channels and information systems

FRAUD– AML SYNERGIES

Synergies between the world of Fraud and AML, with a view to anticipating complex schemes of money laundering and terrorist financing

FULL FUSION

Complete synergies between the Cyber, Fraud and AML worlds, pooling skills, data and technology

EXTERNAL COLLABORATION

Collaboration at the sector level **with peers, law enforcement agencies and regulatory authorities**, aiming at strengthening the security posture and resilience (also at a systemic level) by leveraging on high amounts of data

Establishing external collaboration – The Transaction Monitoring Nederland (TMNL) case

TMNL is a collaboration of five banks to provide faster, better and more effective transaction monitoring

Transaction monitoring in numbers

Five founder banks, NL, 2019

35 million customers

9,8 billion transactions / year

~500 FTE employees

202 thousand alarms / years

The establishment of the TMNL platform has allowed **significant benefits in terms of effective controls and prior identification** of recycling attempts for the various players who participated in the initiative

TMNL objectives

TMNL allows institutions that need to monitor their transactions to centralize most of their activities with the objectives of ...

Streamline the use of (public) resources for criminal investigations

Improving the identification of money laundering and terrorist financing schemes

Protecting the integrity of the Dutch financial system

Promoting (public-private) collaboration in the fight against financial crime

Improve the usability of reporting between banks

TMLN sees a **sub-set of leading banks that have guided the path of establishment of the program**, followed by the additional banks involved in the program

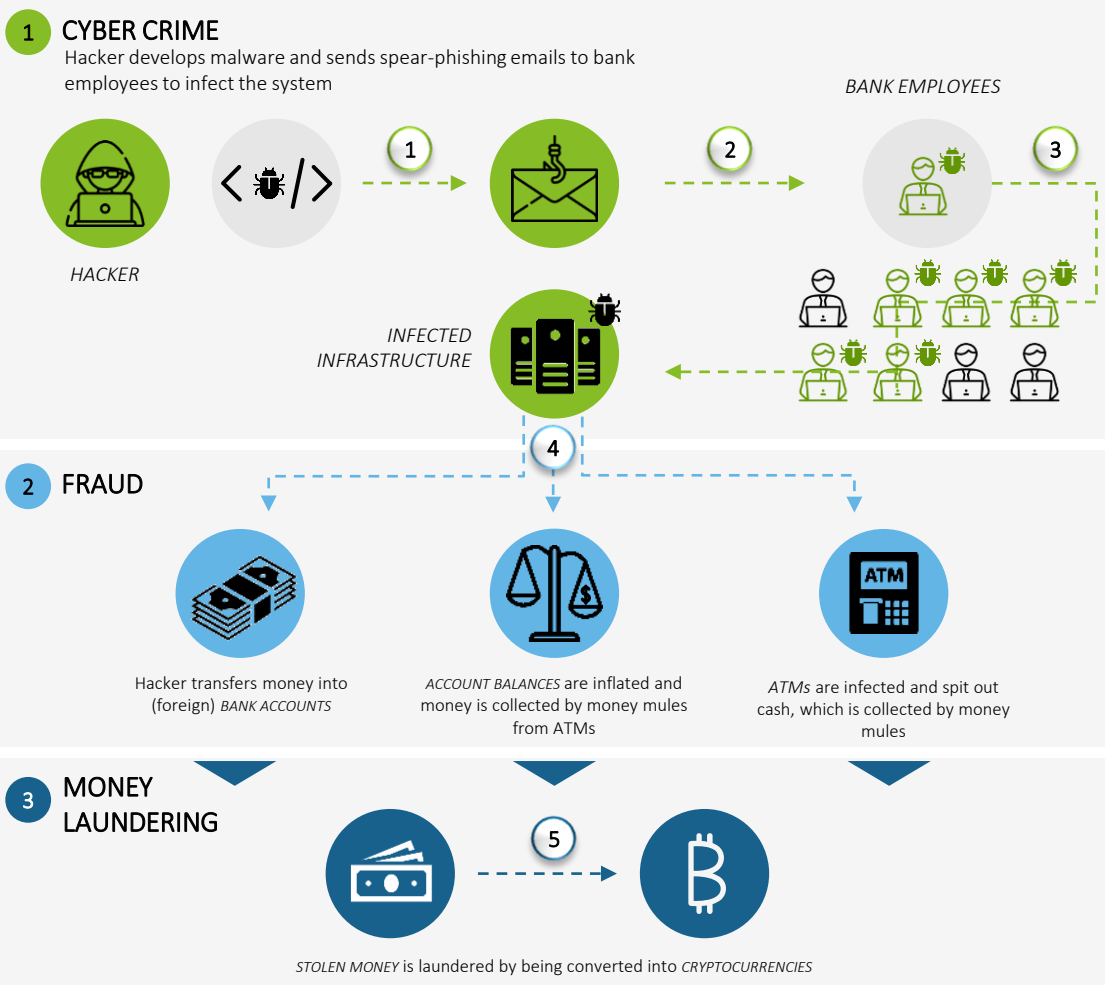

THANK YOU!

Annex

Predicting, preventing and detecting activity across an extended kill chain

Because criminal activities don't recognize our operational silos

The Carbanak / Cobalt case
Anatomy of a computer fraud and money laundering attack[1]



Defence in depth through fusion

1. Cyber SOC is alerted to attempted spear-phishing, content and malware analysis determine malicious payloads embedded in emails

2. Cyber SOC is alerted to endpoint system integrity changes, anomalous user activity and unusual inter-employee communication

3. Lateral spread of malware infection or lateral movement of compromised user account system access and privilege escalation detected in network and authentication logs in SIEM

4. Correlation between anomalies in financial system transactions, compromised privileged user accounts and malware infected servers gives a deeper insight into potential fraudulent activity. Higher fidelity through more data points allows a higher priority to be assigned to mitigate risk by taking preventative measures and introducing additional checks and controls

5. Cyber and Fraud teams raise watchlist to inform internal and external AML teams of misappropriated funds via intelligence sharing. Suspicious attempts to rapidly purchase cryptocurrency is flagged for immediate analysis and potential intervention. Intelligence sharing from external AML investigation teams and enhanced digital risk profiling of beneficiaries provides closed feedback loop to inform Cyber and Fraud teams within fusion centre.

1. Source: Europol - *"Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain"*

Market context – The evolution of AFC approaches

Establishment of a consortium to enhance the presence on specific areas

FRAUD – CYBER SYNERGIES

FRAUD – AML SYNERGIES

FULL FUSION

EXTERNAL COLLABORATION

Cooperation	Geography	Description	Public/ Private-led	Areas considered		
				Cyber	Fraud	FinCrime
Digital Fraud Call	United Kingdom	SME expert call	Private-led	✓	✓	
AUSTRAC	Australia	Mandatory intelligence-sharing FIU	Public- led			✓
JMLIT	United Kingdom	Public-private partnership to combat money laundering	Public- led			✓
FinCEN	United States	Exchange of information on priority threats	Public- led	✓		✓
FMLIT	Hong Kong	Pilot stage typology sharing taskforce	Public- led	✓		✓
CIFAS	United Kingdom	Not-for-profit fraud collaboration	Private-led	✓	✓	✓
Electronic Crime Task Force	European countries	Centralized e-crime response center, with dedicated in-house analysts	Public- led	✓		
European Intelligence Task Force	European countries	Public-private financial intelligence utility	Equal	✓		✓