Integrate cybersecurity, anti-fraud and AML systems for better protection | October 2018

Building a united front on financial crimes

pwc

pwc.com/financialservices

Introduction

In February 2016, the Federal Reserve Bank of New York cleared five transactions by Bangladesh Bank in a single day that totalled more than US$100m. The money was moved to accounts in Sri Lanka and the Philippines. But it turned out Bangladesh Bank hadn't initiated those transfers. Cyber criminals had tricked the system with fraudulent payment requests – and authorities didn't respond in time to stop the criminals from cashing out the accounts. The money sent to Sri Lanka was recovered, but most of the US$81m that was sent to the Philippines disappeared into the country's casino industry.

The Bangladesh Bank heist is just one of several recent high-profile data breaches that have affected hundreds of millions of consumers and that illustrate how attackers exploit weaknesses across the cybersecurity, fraud and anti-money-laundering (AML) operations within financial institutions. These functions are typically organized into distinct silos, which means they have incomplete data, don't communicate well with one another, and repeat tasks and processes.

It is misleading to think of cyberattacks, fraud and money laundering as distinct financial crimes. A dishonest transaction or a cyber-related heist is the front end of a money laundering scheme, because the illegally obtained funds are being moved to some other account. The act of stealing the money – fraud – might take advantage of a weakness in the system's cybersecurity, such as a malware infection on the user device or a phishing attack to steal user credentials. In the case of Bangladesh Bank, the attackers first exploited cyber weaknesses by designing custom malware to bypass controls and network logging systems. They then abused gaps in fraud controls by using the Bangladesh Central Bank's credentials to gain unauthorized access to networks and by setting up fraudulent bank accounts to receive and transfer the stolen funds. Finally, the attackers laundered the stolen money through casinos in the Philippines.

Financial institutions are concerned about cybercrimes, but don't know how best to prevent them. In PwC's 2018 Global State of Information Security Survey (GSISS) and the 21st Global CEO Survey, CEOs and boards named cyberattacks as the business threat they were most concerned about, yet in the GSISS survey, 44% of respondents said they did not have an overall information security strategy. And PwC's Global Economic Crime Survey showed that about half of global firms have fallen victim to fraud in the past two years – a 13% increase since 2016. We believe that for financial institutions to get a clearer view of the threat landscape, quickly identify suspicious transactions and streamline investigations, they'll need to better coordinate their cybersecurity, anti-fraud and AML controls.

What activities can or should be coordinated?

Cybersecurity, anti-fraud and AML programs often have common elements and controls, as well as synergies across people, processes and technology. Most firms are going to find that certain processes should be combined and others should remain separate but share information more closely.

Data management is one of the most critical areas to try to desegregate. One of the reasons cybersecurity, anti-fraud and AML have traditionally operated in silos is that the data sources are in different systems, owned by different parts of the organisation. For example, AML programs might have customers' demographic data and transaction histories, anti-fraud programs might record unusual account activity and changes to account settings, and cybersecurity might collect device, user and network data. Organisations can pool this information into a "data lake" to get a better sense of what is being done on the network and who is accessing which accounts and systems. Threat intelligence from third parties should also be added to the data lake.

Table 1: Where data resides

Data points	Typical owner	Duration of retention/use
User identity information, such as aliases, email address, physical address, phone number	AML, Anti-fraud	Years
User device information, such as IP address, geographical location, manufacturer, operating system, application identifier (or user agent)	Anti-fraud	Months to years
System access (customers and users) events, such as login/logout, failed access attempts, account lockout, password reset	Anti-fraud, cybersecurity	Months to years
Customer/user transaction, payment instruction, service application (e.g., credit or loan)	Anti-fraud, cybersecurity	Years
Data movement, such as by email or file transfer	Compliance, cybersecurity	Months to years
System change events, such as new privileged users or privilege changes, device/application/process starts/stops, changes in software and configuration	Cybersecurity, IT operations	Months to years
Data/file access events, such as create, read, update, delete (CRUD)	Cybersecurity	Days to years

Other areas that financial institutions should consider combining include:

- **Case management:** Money laundering and fraud alerts can be filtered through the same tool (e.g., Actimize, Mantas).
- **Risk assessments:** Cyber, money laundering and fraud risk assessments can be combined to provide a holistic view of an institution's risk.
- **Customer experience:** Although consolidation in this area won't affect financial crime prevention, it can reduce customer friction by eliminating the need for customers to submit the same information more than once or wait for approvals from different areas.

One example of how consolidating activities will help financial institutions is in managing crime prevention at the same time that they explore new technologies, such as faster payments and open banking. Firms will need to be able to push back on suspicious transactions very quickly, because customers expect their payments and other requests to be processed instantaneously. Organisations will need to be able to quickly reference user behaviour patterns, such as the type of mobile device being used, IP address and previous payment history, to assess the validity of payment requests – which will be possible only with the more complete data that results from better information sharing.

Firms will need to be able to push back on suspicious transactions very quickly, because customers expect their payments and other requests to be processed instantaneously.

How can these activities be integrated?

The convergence of financial crime prevention processes can be accomplished only by creating a clear operating model to serve as the backbone for the overall program. An effective operating model consists of a few building blocks: structure, oversight and capabilities.

Structure: Financial institutions should define an enterprise-wide governance model that consists of financial crimes risk committees and charters, escalation protocols, organisational structures, human capital, and staffing and interaction models. This includes formalising – and clearly documenting – roles, responsibilities and communication channels across an organisation's three lines of defense: business units, which are responsible for owning and managing fraud risks; independent risk management functions, which are also responsible for overseeing and managing fraud risks; and internal audit, which is responsible for providing independent assurance for fraud management activities.

When developing this type of governance, financial institutions should consolidate processes, determining which teams can be combined. By organising this way, the institution can detect and eliminate duplicative tasks. For example, instead of having a dedicated team for reviewing escalated money laundering alerts and another for reviewing escalated fraud alerts, a joint group can review both. Better data visibility will make the joint team more effective than having two teams doing essentially the same thing.

As an initial step, firms should consider their existing reporting structure and identify points to streamline so senior management and the board have a centralized view of financial crime risk.

Oversight: Organisations should also adopt an enterprise-wide governance framework to effectively manage the different financial crime disciplines and should establish formalised financial crimes risk committees that support the management, execution and oversight of the cybersecurity, anti-fraud and AML programs. This will enable execution of the overall financial crimes prevention strategy and policy enforcement and will ensure that business units understand and consider the financial crimes risk tolerance when setting strategy. As an initial step, firms should consider their existing reporting structure and identify points to streamline so senior management and the board have a centralized view of financial crime risk. This may mean bringing related activities under the chief security officer umbrella, including cybersecurity, threat intelligence, physical security and anti-fraud.

Also, physical security can play a key role as financial crime systems are integrated, especially by complementing the insider threat programme and further identifying fraud perpetrators. This area is often overlooked for key synergies such as a common case management system, intelligence, law enforcement collaboration and behavioral analytics.

Capabilities: The use of standardised processes and central technology solutions, such as a singular case management system and consistent root-cause analysis, will allow for a coordinated, efficient, easy-to-replicate investigations process. And sharing information among groups will lead to holistic investigations and will force organisations to develop consistent processes within a single framework. This will reduce overall risk. The convergence of AML, cybersecurity and anti-fraud controls provides an opportunity to reexamine how institutions fulfil their regulatory obligations, too, and consolidate those processes.

One size does not fit all

The right solution for each organisation is dependent on several factors, including but not limited to products and services offered, geographic footprint, local laws and regulatory expectations, and customer demographics.

So what actions should firms be taking now?

- Start meeting counterparts in the other financial crimes pillars and initiate discussions around the idea of convergence; uncover short-term benefits, solicit feedback and maintain a dialogue.
- Identify the various technologies and tools being leveraged, and start determining the steps required to move toward more effective solutions.

The path to convergence is not simple or quick, particularly for large and complex institutions. Some opportunities are ripe for convergence immediately, others should integrate in the future and still others should remain separate. What is important is that organisations start a conversation about convergence now.

Contacts

John Garvey
Global Financial Services Leader
PwC US
+1 (646) 471 2422
john.garvey@pwc.com

Paul O'Rourke
Global FS Cyber Leader
PwC Australia
+61 419 109 214
paul.orourke@pwc.com

Sean Joyce
Global Financial Crimes Leader –
US and Americas Cybersecurity
and Privacy Leader
PwC US
+1 (703) 918 3528
sean.joyce@pwc.com

Grant Waterfall
EMEA Cyber Security and Privacy Leader
PwC UK
+44 7711 445396
grant.r.waterfall@pwc.com

Alex Petsopoulos
Partner
PwC UK
+44 07941454210
alex.petsopoulos@pwc.com

Richard Horne
Partner
PwC UK
+44 (0)20 721 33227
richard.horne@pwc.com

Andrew Rosenberg
Manager, Financial Services Advisory Practice
PwC US
+1 (646) 335 4495
andrew.r.rosenberg@pwc.com

Michael Horn
Manager, Financial Services Advisory Practice
PwC US
+1 (646) 471 8052
michael.b.horn@pwc.com

Reema Bagai
Manager, Internal Firm Services
PwC US
+1 (646) 471 8801
reema.bagai@pwc.com

pwc.com/financialservices

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.