KPMG

Battling economic crime — and winning together

How to integrate fraud, financial crime and cyber security to combat threats

KPMG International

home.kpmg/battlingeconomiccrime

Introduction

Long-standing cultural and organizational differences can separate the teams dealing with financial crime, fraud and cyber security. But the line between economic crime and cyber crime is blurring and is already non-existent in the minds of the criminals behind those attacks.

Digital developments, the evolving needs of businesses and customers and the increased sophistication of criminals and their networks, are having a detrimental impact on society and the economy. It requires the forging of a new alliance — one that inevitably demands a holistic approach to combatting a proliferation of threats in this new world.

Highlights

- Convergence between cyber, fraud and financial crime operations to oppose economic crime is fast becoming a new and much needed reality;
- Open and transparent lines of communication and collaboration have become critical;
- Risk governance and threat assessment approaches are aligning;
- Process controls and tooling can be unified to increase their impact;
- A common incident response approach is inevitable.

Contents

Forging powerful new alliances in the war on economic crime

Traditional vectors of economic crime have gone digital to enable the old and new avenues of financial crime, fraud, money laundering and corruption. A new reality has set in for society as economic crime and technology enabled crime become indistinguishable. The result? Experts battling economic crime face the inevitable challenge of aligning their operational capabilities and defenses.

Doing so will require businesses to improve the classic pillars of financial crime, fraud and cyber security governance, forging for the future a more holistic, overarching approach to economic crime that's rigorous, comprehensive, effective and resilient. In the face of criminals endless pursuit of new and creative ways to make money, future operational defenses must also be ever evolving.

Similarities

While individual cyber security, fraud and financial crime teams have changed with the times in response to unprecedented new challenges, they continue to share similarities in the digital era. Cyber security teams are managing information security, technology resilience and some aspects of data privacy controls. The focus of today's financial crime teams, predominately, includes anti-money laundering (AML), anti-bribery and corruption (ABC), anti-tax evasion and sanctions monitoring. And fraud's remit extends to insider threat and financial fraud activities such as social engineering, credit or debit card fraud and money mules transporting currency illegally. Each of these teams are dealing with the same issue: organized crime intent on profiting from illegal activity perpetrated by access to systems, from stolen information and from manipulation of vulnerable people.

In more mature organizations, the operational environments between financial crime (typically regulatory driven), fraud (business driven and concerned with monetary loss and customer security) and cyber are converging, with shared data, analytics, insights and technology being deployed to work on key threats together.

The changing ecosystem

Cyber security governance reflects aspects of both fraud and financial crime. Mirroring financial crime regulations on money laundering, bribery and corruption, regulators are increasingly holding organizations accountable for the cyber resilience and data privacy controls of their supply chains and a growing ecosystem of partners.

Fraud and cyber security, meanwhile, address extremely similar threats and are evolving along similar lines. In both areas, regulators, especially in the financial sector, are increasingly placing the onus on organizations to adequately protect customer finances and access to financial and e-commerce applications.

For all three disciplines, the lines between management of enterprise and supplier risk are falling away as supplier ecosystems grow more complex and interdependent. And as consumer expectations for security grow, all functions are becoming increasingly tied to protecting brands and reputations.

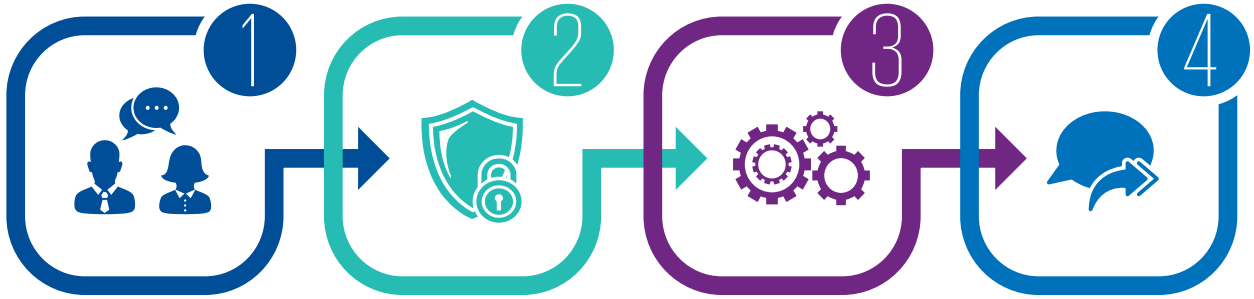
Innovative teams demonstrate winning game plans

As with fraud and financial crime, some financial institutions have been testing the waters by linking these operations with cyber teams. One bank has combined fraud predictive analytics tools and cyber security intelligence to detect internet protocol (IP) addresses and payment patterns, thus identifying mule accounts and preventing money laundering.

In another case, IP addresses were used to track down a criminal network exploiting e-commerce platforms to test stolen credit cards and e-wallets. The investigation that caught them included fraud, financial crime/money laundering and cyber teams.

These use cases are indicative of the emerging direction of travel towards a data- and technology-led strategy, which aligns cyber security, fraud and financial crime operations to more effectively and efficiently manage the detection and disruption of criminal economic activity.

Four steps to aligning and converging financial crime, fraud and cyber security



At a higher level, organizations should be thinking about the steps they can take to partner and collaborate with peers to actively defend their ecosystem from a converging set of economic and cyber crime activities.

Step 1: Improve communication lines and collaboration

Cross-train each other in terminology and business/ regulatory environments

Financial crime and fraud teams communicate using language and jargon that at times can sound foreign to cyber teams, whose own high-tech talk about malware and attack vectors can mean little to fraud investigators. Cyber and financial crime/fraud teams need to find a common language — as they are ultimately targeting the same criminal networks. Cross-training between teams can address some of the terminology gaps and ensure that each team is familiar with the others' drivers and business settings.

Establish multi-disciplinary points of contact in each team

Each financial crime, fraud and cyber team should include at least one member possessing a firm knowledge of the other fields. Include multi-disciplinary skills as a requirement during recruitment and upskill existing personnel through secondment and rotational programs.

Hold joint team meetings and conference visits

Cyber, fraud and financial crime teams should host joint team meetings to discuss common challenges, regulatory pressures and business drivers. Look for common cause in targeting an aspect of economic crime. Cyber and fraud teams should ensure that representatives of their respective teams attend relevant security or fraud conferences to increase awareness of the diverse threat landscapes.

Break down the silo mentality and develop cross functional ways of working

Allow staff to flexibly move between operational teams to break down the silo mentality, and enable joint investigative teams to collaborate by selecting staff with the right skill sets and experience.

Develop cross functional ways of working with the right mindset and expertise to operate across the domains.

Step 2: Align and link approaches to risk and threat assessment

Map industry best practice standards and regulations

Cyber security best practice is governed by a range of security standards and commonly used frameworks which are now being reflected in financial audit legislation, privacy regulation in various jurisdictions, and regulation of critical infrastructure resilience. Financial crime and fraud teams also apply industry best practice and standards to their operational frameworks. There is an opportunity to bring together relevant standards in an enhanced risk assessment framework, which more accurately resembles the change in patterns and behaviors of criminals and how they perpetrate their crimes. For example, financial crime and fraud teams could map relevant regulations and fraud's 'Prevent, Detect, Respond' framework to cyber security practices such as the NIST cyber security framework to develop a common standard for internal audit and risk assessment.

Establish an enterprise-wide risk assessment framework

Cyber, fraud and financial crime teams pursue different approaches to identifying, documenting and rating risks across multiple areas. In regulated industries such as finance, enterprise-wide financial crime risk assessments are a requirement. These cover customers, delivery channels, transactions, third parties, staff and industries or jurisdictions. In many organizations, operational risk frameworks can require risk assessments to be completed independently for each function.

At an operational level, a more comprehensive approach to identifying and mitigating economic crime threats should see risk assessments cover fraud, cyber security and some aspects of data privacy, alongside the financial crime focus. Teams should develop a unified risk and control framework that identifies common risks and effectively addresses them.

Develop joint working groups and key performance indicators on common threats

While each team may continue to report into different governance lines, financial crime, fraud and cyber should develop common risk metrics that can be used to track and respond to common threats, and facilitate joint operational task forces as they align working practices and collectively engage the wider business on shared challenges.

Step 2: Combine and link approaches to risk governance and threat assessment (cont'd)

Conduct unified threat assessments and regulatory horizon scanning

Financial crime, external fraud and cyber attacks are often perpetrated by organized crime using criminal networks at scale, with internal fraud or insider security threats also motivated by the same group of people. Changes to the modus operandi of criminal networks, and the regulatory landscape, can have implications for all three functions at the technical control level.

Financial crime, fraud and cyber security teams should consider undertaking joint threat assessment workshops with business units to collectively identify threats, share threat intelligence sources and outputs, and store relevant threat intelligence in a single, unified repository. Each team should ensure that the relevant outputs of regulatory horizon scanning are also shared.

Step 3: Unify data, process controls and tooling

Exploit data driven predictive fraud risk controls in cyber

The risk of money laundering and bribery and corruption increases for business operations, roles and suppliers in certain industries and jurisdictions. It's good practice to maintain a list of higher risk jurisdictions and industry sectors. You can also use external sources such as national risk and threat assessments and lists from NGOs, such as *Transparency International's Corruption Perception Index*, to supplement internal risk assessment and categorization. These sources can also be used to take a risk-based approach to security controls or predict exposure to technology enabled crime for new business ventures and projects in certain jurisdictions.

Cyber teams looking to be proactive in risk management should consider how to modify, based on fraud and financial crime risk indicators, security monitoring controls, access approvals and application security requirements.

Examine how financial transactions performed by higher risk suppliers, staff and IP addresses can be integrated into such risk frameworks and put under enhanced control environments.

Identify opportunities to unify prevention and detection tooling

Cyber security teams employ a range of tools for privileged user monitoring, network traffic inspection, data loss prevention, dark web monitoring, security incident and event monitoring (SIEM), and malware detection.

Fraud and financial crime teams have an opportunity to embed their intelligence into the cyber threat intelligence team's analysis of likely cyber attack techniques, including their monitoring of higher risk users and their associated activities. Can the fraud team provide insights which help configure security defenses (for example email and web filtering, and data loss prevention controls)? Can analysts looking at security alerts benefit from a better understanding of financial processes which might be manipulated to commit fraud?

Cyber teams should also understand the capabilities of data driven fraud analytics engines and consider how best to apply them for both fraud and insider threat management. For both functions, the unification of tooling suites can enable fraud and cyber crime prevention, reducing the need for post-incident forensics and recovery.

Step 3: Unify data, process controls and tooling (cont'd)

Develop a unified services architecture for products and service delivery channels

Businesses typically offer a multitude of digital services to their customer base via diverse digital channels. These have different onboarding requirements, backend security arrangements and approaches to handling fraud. For financial services organizations, this has created difficulties in obtaining a single customer view, plus disjointed methods of operating, monitoring and securing each service or channel.

Creating a single integrated view of customer interactions across product channels, leveraging a data-led approach, can simplify development of consumer products and deliver more consistent, holistic insights to financial crime, fraud and cyber teams monitoring them.

Embed fraud and financial crime controls into secure DevOps

Cyber security teams seeking to embed agile security into software and application development operations (DevOps) should understand how fraud and financial crime controls can also be integrated into development.

As customer expectations for financial applications and transaction security grow, promoting a 'trusted-by-design' approach — one encompassing fraud and financial crime into 'secure-by-design' philosophies — may improve customer loyalty and build partnerships within the business.

Integrate controls across end-to-end customer lifecycle management

Even as consumers seek less intrusive financial and security controls on products and services, effective defenses against financial crime, cyber attacks and fraud are becoming more closely linked to an organization's brand and customer loyalty.

All three teams should occupy front line positions in their business, supporting customers by embedding seamless customer authentication and identity verification mechanisms into consumer facing products and services, while also minimizing the impact on customer experience. These can include risk based, behavioral authentication methods and machine learning powered recognition technologies. At the KPI level, metrics around customer security controls should be integrated with those of financial crime and fraud.

Step 4: Establish a common incident response approach

Integrate the service desk to provide incident management across all functions

Driving a coordinated response to incidents is often complicated by the lack of a single service desk channel. Does your business have separate monitoring and reporting channels for data loss, fraud, financial crime, cyber attacks and IT issues? Are there separate channels for internal, external and customer facing incidents, even though events may be closely linked? Are instances of fraud, data breaches and malware activity managed through independent escalation lines, even though each may be different elements of the same attack?

Organizations should consider integrating service desks to improve stakeholder and resource alignment, response times and real-time data provision, and to ensure that incidents are understood end-to-end, from trigger points at the customer or employee level to their appearance on SIEM tools and eventual closure.

Align playbooks for cyber, fraud and financial crime incident response

Cyber incident playbooks detail how security operations center (SOC) teams respond to specific use cases, such as distributed denial-of-service (DDoS) attacks, ransomware, abuse of privileges and data loss.

Financial crime and fraud teams undertake threat assessments for focused and prioritized threats. There is an opportunity to combine the expertise and intelligence on playbooks and threat assessments to streamline the approach and ensure a more holistic assessment is undertaken thus ensuring certain threats are better triaged, managed, investigated and disrupted. This not only helps streamline the approach but can also better define requirements around customer compensation and regulatory notification.

Conduct joint red/ purple teaming activities

Cyber security teams utilize third parties to conduct red/purple teaming exercises, in which incident detection tools, response playbooks and security teams ('the blue team') are tested by a simulated threat actor (the 'red team') in an adversarial setting.

There may be scope to include fraud and financial crime teams in red/purple teaming activities, to test fraud incident playbooks, understand if detection tools can effectively detect fraud and financial crime activity, and to ensure that response processes are up to scratch.

Step 4: Establish a common incident response approach (cont'd)

Jointly conduct retroactive lessons learned activities following incidents

A time worn challenge of incident response is understanding the full sequence of events that allowed an attacker to compromise a network or beat prevention controls. Ensuring that post-event lessons learned activities include both consumer facing, internal fraud and information security teams is critical to creating a revealing holistic view of the incident.

What can you learn from the other team? What parts of the control framework do they have visibility over that you don't? Understanding the end-to-end compromise scenario can enable teams to efficiently remediate control gaps at the right point.

Actively defending your ecosystem

Enacting these innovations within an organization demands vision and leadership, and a willingness to test new ideas and ways of working linked to a pragmatic approach which looks for early business benefits in countering criminality.

But it is worth remembering that cyber attacks and economic crime are systemic challenges that require industry-wide action to effectively combat them. Extending the integration of cyber security, financial crime and fraud into the larger ecosystem — your network of suppliers, partners, regulators and competitors — is a step in enhancing trust and countering crime.

Addressing the 'cyber poverty line'

Cyber threat actors, fraud perpetrators and organized crime are often intricately linked and mutually dependent. When organizations possess strong cyber security, fraud controls and response processes, threat groups are inclined to shift focus to target less capable organizations, hitting below what the World Economic Forum's Center for Cybersecurity refers to as the 'cyber poverty line.'

There is mutual benefit in organizations with the strongest capabilities working with government and law enforcement to actively hunt threat groups, rather than passively defending against their assaults on a reactionary basis.

The most mature organizations are gathering technical intelligence on fraud perpetrators, cyber threat groups and organized crime when they attack and using it to assist law enforcement with the disruption of those groups including the identification and arrest of suspects. Organizations should also work with supply chain partners, including incident response providers and security operations centers (SOCs), to gather critical data on threat actors.

Collaboration within industries

Public-private partnerships are in place in a number of jurisdictions for both economic crime and cybercrime. Efforts should be expanded and deepened, with protocols developed to enable ecosystem wide intelligence sharing and collaborative threat hunting, coordinated in part by law enforcement and industry groupings. Collaboration between industry peers is critical to effectively combat the social harm caused by cyber and financial crime, including fraud. This new way of working collaboratively and in partnership demands an enhanced level of transparency between organizations and law enforcement as well as support from their

regulators and competitors to ensure that together they combat larger scale attacks on industries and supply chains — attacks that smaller organizations are unable to repel alone. Governments have a key part to play in enabling the legal and operational framework for this co-operation to flourish which protects the privacy of citizens while countering crime.

Active defense techniques, ranging from pre-emptive detection, offensive 'hack backs,' deception and disruption, have been increasingly deployed in cyber space over the last decade. In many cases, partnerships between private organizations and public agencies have been critical to their success.

Botnets disrupted.
A major technology provider collaborated with US Cyber Command to feed false information to known malicious ransomware groups, disrupting their botnets[1].

Poisoning a network.
One US educational institution worked with law enforcement to 'poison' the Tor anonymity network and unmask user identities on a well-known darknet market[2].

Partner data.
INTERPOL has used data collected by a private sector partner to identify a strain of malware infecting e-commerce sites to steal payment card details and personal data. Intelligence gathered was disseminated to affected countries and led to the arrest of three cyber criminals in Indonesia[3].

At a strategic level, the UK's National Cyber Security Centre (NCSC) has implemented its Active Cyber Defense (ACD) program to reduce the impact of commoditized cyber attacks against UK markets. There are also emerging examples of active defense models in some corners of the economic crime space, with public and private partnerships combining intelligence and capabilities to increase response effectiveness.

In the UK financial services sector, the Joint Money Laundering Intelligence Taskforce (JMLIT), a partnership between regulators, law enforcement and the financial sector, has driven significant successes since its inception in 2015 and is considered internationally to be an example of best practice. As a community of fraud, financial crime and cyber security practitioners, we need to ask ourselves what opportunities exist to extend successful defense models against a wider set of digital threat groups and modus operandi.

[1] Andy Greenberg, *A trickbot assault shows US military hackers' growing reach*, Wired.com, October 14, 2021.

[2] Andy Greenberg, Tor says feds paid $1M to help unmask users, Wired.com, November, 11, 2015.

[3] INTERPOL supports arrest of cybercriminals targeting online shopping websites, INTERPOL, 2020.

Prepare for a complex new threat horizon

Active defense helps us counter the threat vectors of today and eliminate in the longer term some of the groups that perpetuate cyber and fraud campaigns. But as technology capabilities advance, cyber and fraud attacks are becoming dramatically more commoditized and scalable. The cyber security and fraud threats of the next decade will be profoundly enhanced by emerging technologies and propagated through complex supply chains and working models.

Bringing together cyber, fraud and financial crime operations within organizations, underpinned by a holistic data strategy, is an excellent start to meeting the challenge. At the ecosystem level, addressing a commoditized threat landscape will require further investment into a coordinated, industry-wide response that is able to target and disrupt serious and organized crime.

How KPMG can help

At KPMG, our global organization of cyber security, financial crime and forensic professionals offer a multidisciplinary view of risk. Helping you to protect your organization, so you can anticipate tomorrow, move faster, and get an edge with secure and trusted technology.

KPMG brings an uncommon combination of creative professionals, strong business insights and deep technical expertise that can help introduce new levels of resilience and agility to your cyber security, fraud and financial crime governance. Together, we help create a trusted digital world, so you can push the limits of what's possible.

Our authors

David Ferbrache
Global Head of Cyber Futures
KPMG International

Dani Michaux
Cyber Security EMA region Lead, Head of Cyber Security in Ireland and Partner
KPMG in Ireland

Geraldine Lawlor
Global Head of Financial Crime, Partner
KPMG in the UK

Alexandra Anisie
Director, FS Cyber
KPMG in the UK

Bettina Kuntz
Senior Manager, FS Forensic
KPMG in the UK

Steven Ackroyd
Senior Manager, FS Forensic
KPMG in the UK

Ravi Jayanti
Assistant Manager, FS Cyber
KPMG in the UK

Contacts

Akhilesh Tuteja
Global Cyber Security Leader, Partner
KPMG in India
E. atuteja@kpmg.com

David Hicks
Global Head of Forensic, Partner
KPMG in the UK
E. david.hicks@kpmg.co.uk

Geraldine Lawlor
Global Head of Financial Crime, Partner
KPMG in the UK
E. geraldine.lawlor@kpmg.co.uk

Natalie Faulkner
Global Fraud Lead, Partner
KPMG Australia
E. nfaulkner1@kpmg.com.au

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name: Battling economic crime — and winning together
Publication number: 137178-G
Publication date: December 2020