Staying ahead of cyber crime

UK FINANCE

April 2018

KPMG

UK Finance

UK Finance represents nearly 300 of the leading firms providing finance, banking, mortgages, markets and payments related services in or from the UK. UK Finance has been created by combining most of the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association. UK Finance has an important role to play helping negotiators understand how the interests of UK and EU customers, and the financial services they all depend upon, can be best protected. Our members are large and small, national and regional, domestic and international, corporate and mutual, retail and wholesale, physical and virtual, banks and non-banks. Our members' customers are individuals, corporates, charities, clubs, associations and government bodies, served domestically and cross-border. These customers access a wide range of financial and advisory products and services, essential to their day-to-day activities. The interests of our members' customers are at the heart of our work.

www.ukfinance.org.uk

KPMG

At KPMG, we believe in proactively incorporating cyber risk management into all activities. Cyber security is not just a reactive technical fix – it can also be a driver of change and secure the future of your business.

With over 2,000 security practitioners world-wide, KPMG can give you the support and guidance you need to adapt to new global threats. By evaluating business resilience, optimising the relationship between people, process and technology, and bringing the latest industry insights, we can help turn risk into advantage.

KPMG in the UK employs 12,000 people across 22 offices in the country and we are part of a global network operating in 155 countries around the world. Providing audit, tax and advisory services we combine our multi-disciplinary approach with deep industry knowledge to help clients meet challenges and find opportunities each and every day. The independent member firms of the KPMG network are affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. Each KPMG firm is a legally distinct and separate entity.

Table of Contents

Foreword

Cyber security is now second only to political risk as one of the key challenges facing the UK financial sector. Cyber crime has become big business, with the global impact exceeding $450 billion a year as crime, extortion, blackmail and fraud move online.

To be effective in addressing this risk, the approach of businesses across all sectors needs to change to a community-based and comprehensive approach to disrupting the criminal ecosystem. This demands that we understand the threat from the perspective of ruthless and rational cyber criminal entrepreneurs, and that we work together across the financial community, key industries, law enforcement and governments to break their business models.

It isn't simply a question of spending more money on more robust security systems: banks alone spent $360 billion on IT in 2016, and financial services firms already spend three times the amount that non-financial organisations do on cyber security. This growing challenge demands new ways of working between government, law enforcement and the finance industry, but most critically a shift to new security models that are agile, responsive and focus on protecting customers against exploitation.

No single organisation can achieve this in isolation: we must work through effective partnerships to tackle this scourge of our digital economy.

Bill Michael, Chairman
KPMG in the UK

Stephen Jones, CEO
UK Finance

Are the criminals winning?

Cyber crime is displacing conventional crime. As our world has become digital, so has our money, and crime follows the money.

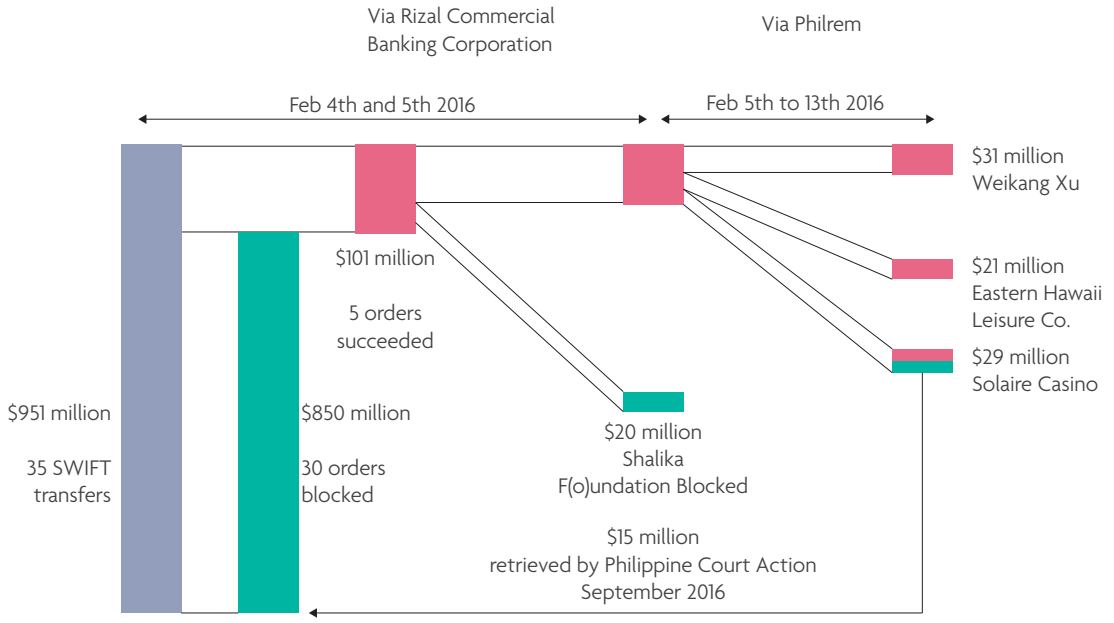
Much of the focus of the debate on economic crime has rightly been on the impact of cyber-enabled fraud on consumers and businesses. However, there is also a growing trend for criminals to target the systems and operating software of businesses, governments and key infrastructure in a coordinated and systematic manner.

Organised crime attacks the financial community as a whole, and criminals are becoming increasingly sophisticated in finding and targeting weak points across this community, supported by a black market in stolen personal information and in 'crime as a service'. Extortion attacks are also alive and well in the form of ubiquitous ransomware, while criminals now attempt protection rackets by threatening to carry out large-scale denial of service attacks against firms' online portals.

Cyber criminals are demonstrating a growing knowledge of our financial systems and the potential weaknesses. There is a worrying trend towards more targeted attacks, with a growing knowledge of how these systems work and how to cash out.

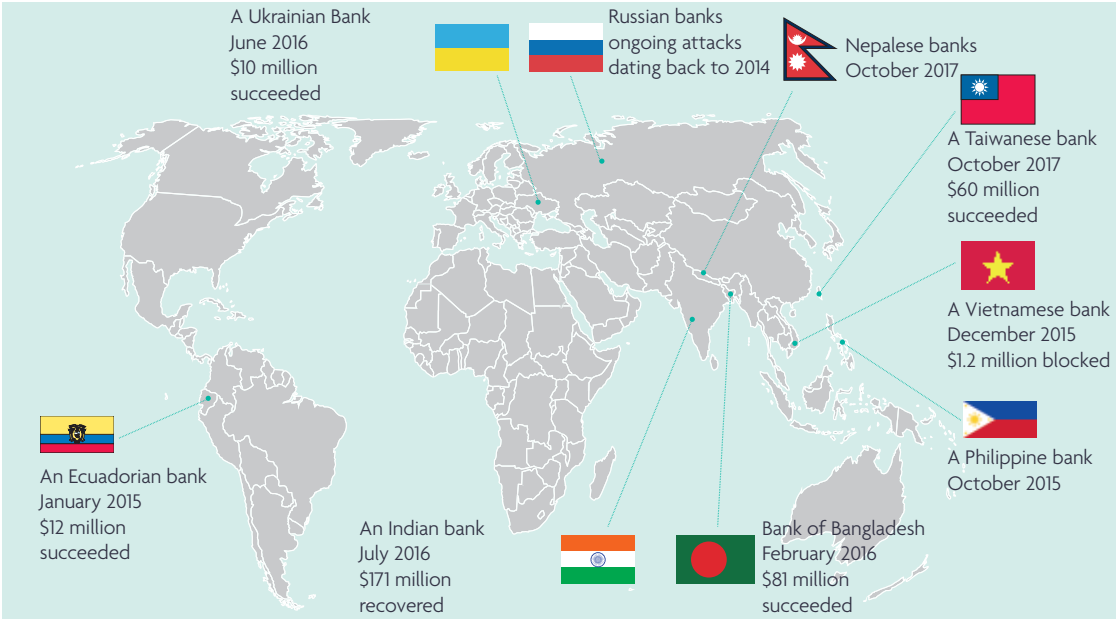
It is perhaps time to ask ourselves what we, as a community, should do to stay ahead of those intent on committing cyber attacks against the UK financial services sector.

Case Study: Bangladesh Bank



The 2016 attack on Bangladesh Bank involved a compromise of the central bank's IT systems, allowing attackers to manipulate the payment gateway connecting the bank to the SWIFT worldwide international financial transaction system. The attackers were able to submit 35 fraudulent payment transfer requests aimed at moving money to Sri Lanka and the Philippines, although all but five of these were blocked by anti-money laundering and fraud controls.

This high-profile incident was just one of a number of attempted cyber attacks aimed at manipulating bank payment systems over the last three years. Many of these attacks used a similar modus operandi, involving targeted phishing emails often purporting to come from the central bank or from the SWIFT system itself. These were followed by compromises of the bank systems over a period of many months, allowing attackers to become familiar with the bank security defences and best cash-out channels.



We don't think like they do

Perhaps our 'achilles heel' is that we don't think like criminals.

Do we really understand how criminals operate? Do our security measures really make their lives harder and their business less profitable and more risky?

The criminal mind-set can be very different to that of our security professionals.

Criminals focus on cash-out, exploitation and making money. They are prepared to use every method at their disposal to extort, blackmail and defraud. They don't care about internal organisational structures and are happy to exploit the gaps in the way financial firms and global businesses work together. They continuously innovate their attack tools and techniques. They work as part of a criminal ecosystem trading information and offering crime as a service. They are not constrained by the rule of law.

Financial institutions, as highly regulated entities, focus on controls, structures, processes and technology. The security response of firms must be managed through carefully controlled and audited control environments, delivered at the pace that this verification and accounting process allows.

One challenge the industry must address is not to see cyber security as merely a governance, risk and control issue, but as a matter of competition with a digital adversary.

In many respects, the way businesses approach identifying and harnessing digital channels to market is much closer to the business models adopted by criminals. Businesses continuously evolve their market offerings, looking for new opportunities. They test new routes to market, and do so at pace in order to create competitive advantage.

Two very different business models

Organised Crime	Financial Institutions
Agile and continuously evolving tactics and techniques	Highly regulated systems and processes can get in the way of innovation
Flexible and adaptable infrastructures exploiting cloud technology	Invest to ensure legacy systems are fully protected or maintained
Market economy in information and crime as a service	Legal constraints get in the way of information sharing
Pragmatic collaboration to achieve win-win outcomes	Cooperation often driven by personal relationships
Operate transnationally outside the law or regulation	Operate within the law and regulatory direction in their jurisdictions
Able to recruit and reward success – occasionally punishing failure	Skills shortages can prevent access to best talent

How are we addressing the ever - changing challenge?

The value of coordination and cooperation is increasingly seen as key to future cyber capability development:

COLLABORATION is allowing organisations to improve cyber defences by sharing good practice and insights from individual experiences and lessons learned from incidents and attacks. Knowledge exchange for both individuals and corporate culture will generate the continuous improvement vital to meeting the challenges of responsive and dynamic threat actors and threat networks.

FEDERATION is the collective defence of digital eco-systems that recognises electronic commerce, reliant on hyper inter-connectivity, presents a dimension of interdependency that cannot be addressed by a digital fortress mentality alone. Bold, pioneering and innovative federated cyber defence capabilities are beginning to emerge in the UK. However, further capability development is required to realise the full potential and secure digital eco-systems across the business community and the supply chain.

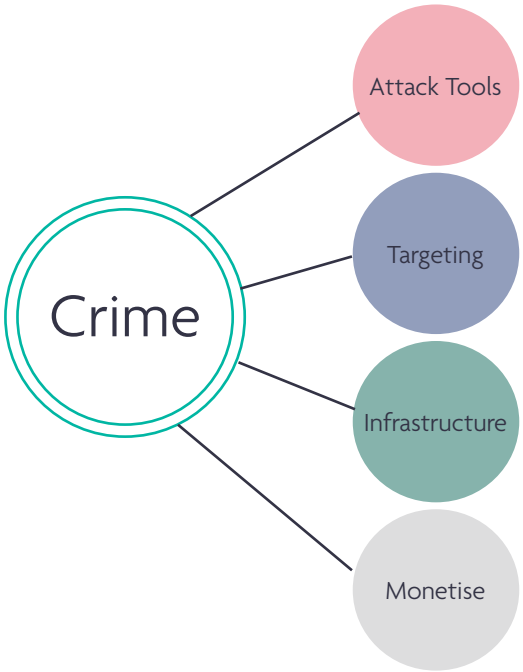
INTEGRATION is both across business partners, but most notably between the public and private sector. This will be key to disrupting current and future cyber-threat networks. The active defence of these eco-systems will require the development of analytical capabilities that afford insight and foresight of those seeking to attack our businesses and markets. The establishment of the National Cyber Security Centre (NCSC) is testament to the public sector commitment to integration, but can only ever be part of the answer.

In short, the ethos of 'build a network to defeat a network' recognises both the character and nature of the threat networks whose enduring capability and intent represents a significant threat to digital commerce and society. This is far-reaching, and affects policy, legislation and regulation as well as the skills that will be required to meet this novel and complex challenge of the 21st Century.

How do we do more to put them out of business?

To effectively address the growing threat of cyber-criminals, the financial services industry needs to work more effectively to make the cyber criminals' 'business model' less profitable; by reducing their revenue, increasing their cost base, or making their operations riskier.

Fig 1: Crime as a service



To achieve this, the financial services industry, working with law enforcement and government, must build on existing work and initiatives, as follows, to better address these challenges:

- Reduce the success levels of the cyber criminals' attacks on firms' systems by improving security defences across the community.
- Increase firms' ability to detect criminal activity. This would enable firms to block activity and respond more quickly to any security breach or data theft, reducing the time criminals are able to access systems and minimising the window of opportunity to steal and exploit data.
- Disrupt the infrastructure used by criminals. This would help to render ineffective the markets, tools and systems used to conduct criminal activity.
- Better block the exploitation of stolen data – detecting data losses or compromises, and revoking stolen credentials or priming fraud controls, to detect the use of stolen data.
- Prevent cash-out and money laundering, further tailoring fraud and anti-money laundering controls to reduce the likelihood of the criminal group benefiting from their actions.
- Increase the risk to the criminals. This can be done through promoting cooperation and public-private partnership between governments, the private sector and across the law enforcement community, and will maximise the chance of arrest and prosecution.

Disrupting their business model

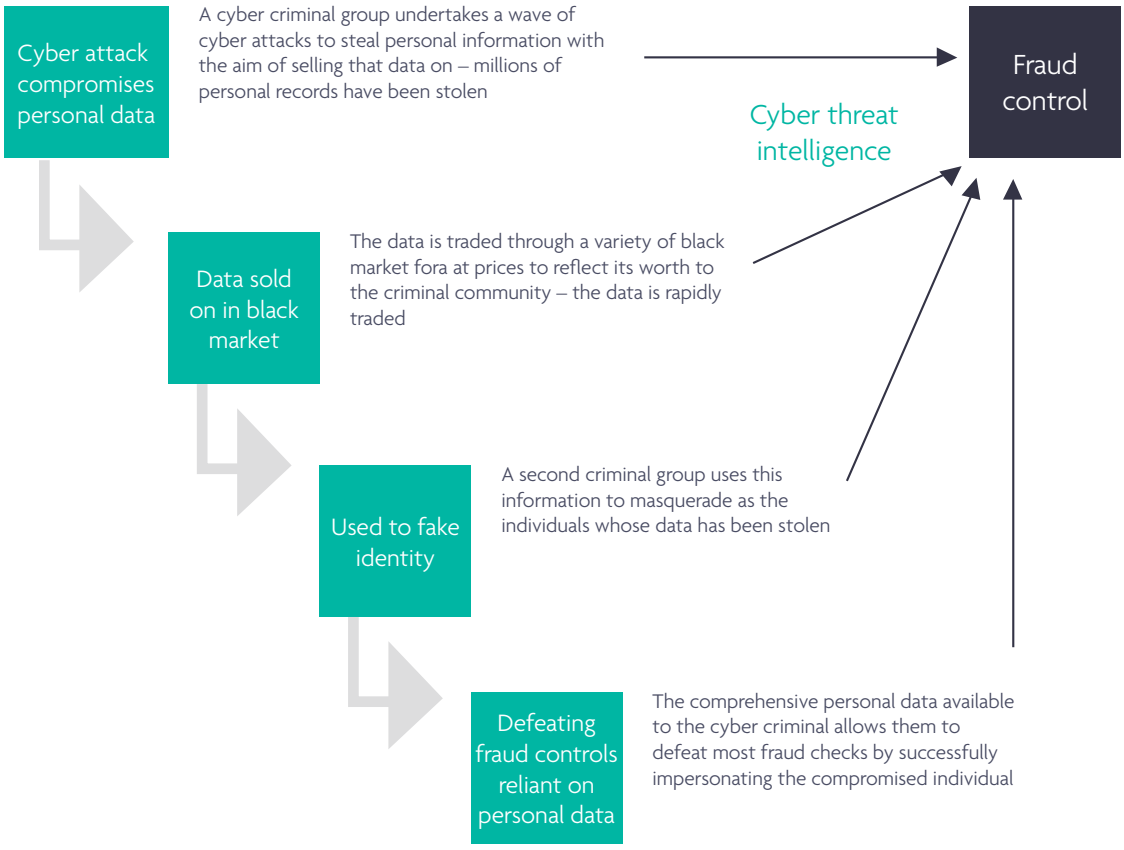
Fig 2: An agenda for community action

Time for greater cooperation within businesses

The approach of the financial services industry to countering economic crime is diverse and complex. In tackling economic crime, banks in the UK currently spend £5 billion annually on compliance (including customer due diligence, transaction monitoring, sanctions and fraud risk). These more traditional economic crime and compliance functions can often be distinct from the processes that authenticate customers using digital channels, and secure those digital channels and the core banking systems they interact with.

A key challenge for firms is to ensure these important control and compliance functions (and the teams who run them) are not viewed in isolation. Firms must ensure functions work together to detect and block the attacks used by cyber criminals, as well as help interdict their cash-out and monetisation.

Fig 3: Understanding the nature of the threat to improve controls and coordination



Time for greater collaboration...

Cyber criminals adopt a broad approach to targeting. From commoditised attacks such as ransomware that strikes every organisation, to the most targeted attacks seeking weak points in our financial system, multiple institutions are being attacked and the compromise of one may provide an 'in' to attack other peers, customers or suppliers.

It is clear we need a community response to cyber crime that matches the agility and market structures employed by cyber criminals.

The information-sharing structures operating across the financial sector are still developing. The establishment in 1999 in the US of the Financial Services Information Sharing and Analysis Center (FS-ISAC) represented a major move to improve collaborative sharing. This was followed by FS-ISAC initiatives to automate information exchange in 2014 and the creation of the Financial Systemic Analysis and Research Center in 2016, bringing key banks together with the US government and law enforcement community.

In the UK, the government created a Cyber Intelligence Sharing Platform (CISP), complementing the Financial Services Information Exchange the government had previously operated. A number of the major banks also came together to form the Cyber Defence Alliance in 2016, providing a collaborative intelligence analysis environment.

As a community, we now need to scale our response in a way that recognises the breadth of the financial services sector and grows interdependency and inter-connectedness across that sector.

When faced with a tsunami? Build an ark!

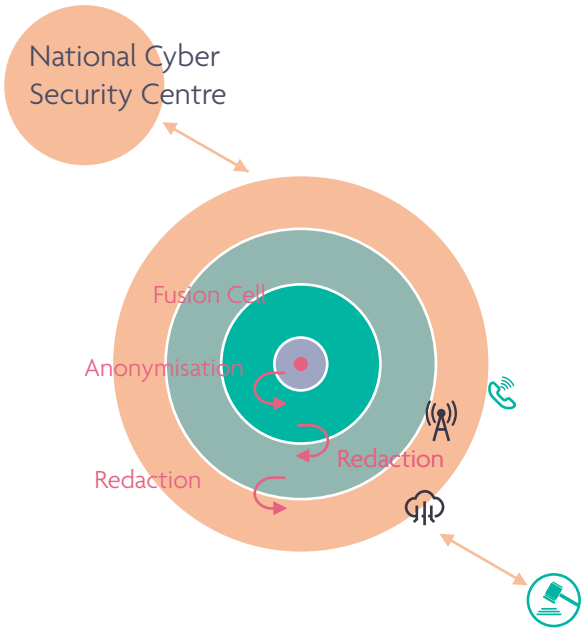
On 24 October 2016, eight US banks announced that they were establishing the Financial Systemic Analysis & Resilience Centre (FS ARC) to enhance the protection for US FS critical national infrastructure. The FS ARC represents an inner core to the wider Financial Services Information Sharing and Analysis Center (FS-ISAC), which was established in 1999 in response to a US presidential directive, and recognises that systemically important financial institutions need greater situational awareness. This small community of action allows a rapid response to cyber attack campaigns against individual institutions and key elements of the US financial services sector. The US FS ARC represents the most sophisticated example of a capability that evolved from the experience of the principles of COLLABORATE–FEDERATE–INTEGRATE.

What should we do next?

We must recognise the range of skills and capabilities within the financial services sector: from large global banks with considerable cyber threat intelligence and forensic resources, to smaller institutions that may be dependent on a more modest security team supported by third-party security advisers or service providers. All have a contribution to make, and any could become the target for cyber crime.

This leads to a layered approach in which institutions choose their level of commitment and integration into a community intelligence sharing and action model – but with a clear undertaking to support the broader community by summarising and sharing the results of their analysis. In part, these choices will be driven by the maturity of their own cyber threat intelligence, forensic and cyber defence capabilities, and their ability to contribute and act.

Fig 4: A proposed model for cyber security federation



Inner Community of Action
FIs/FMIs central to financial markets and eco-systems with full spectrum cyber defence able to deliver comprehensive capability and capacity to develop insight and foresight from security intelligence and threat intelligence.

Outer Community of Action
Significant FIs/FMIs to financial markets and eco-systems with broad cyber defence able to deliver comprehensive capability to develop insight and foresight from security intelligence and threat intelligence.

Business Community of Interest
FIs/FMIs to financial markets and eco-systems with regulatory required cyber defence, but with limited capability and capacity to develop insight and foresight from security intelligence and threat intelligence, but who nonetheless represent an interconnectivity and interdependence risk.

Supply Community of Interest
Key enablers and essential services to the market or FS eco-system that represent a key dependency risk

While this layered model seems attractive, we must also recognise that the financial services sector is not homogeneous and nor are the threats. It is likely that 'hubs' will develop in different communities, reflecting their very different composition and in some cases the different cash-out and exploitation methods adopted by criminals.

We need a joined up approach

While this model can help address threat intelligence sharing, much more can be achieved by close cooperation with the NCSC (enabling more active steps to disrupt the infrastructure used by organised crime groups), and with the National Crime Agency (NCA) and police forces, such as the City of London police, to investigate and prosecute criminality.

Only by breaking down the barriers between the cyber security, fraud and financial crime disciplines can we really hope to counter cybercrime. We need to be prepared to think like a criminal, and that demands a multi-disciplinary approach to countering crime which focuses on disrupting the criminal's business model, quickly and effectively.

Now is the time to act

Cyber-attacks have the capacity to act as a drag on our economic growth, whether it be through loss of trust in our digital infrastructure or the direct losses that follow fraud and extortion.

We need to demonstrate an agility of approach and mind-set to counter the growing cybercrime threat. We must be prepared to challenge our own security defences using the mind-set of an attacker, be willing to harness diverse skills and innovation in the way we tackle security and avoid the trap of over-reliance on compliance-driven, inflexible and stovepiped approaches to such a rapidly changing threat.

Without action to address this threat as a community, we risk directed regulatory action that may ultimately prove counter-productive in reinforcing that compliance-driven and risk-averse culture. A culture which will ill prepare us to deal with a rapidly changing cyber threat.

Worst of all, that breakdown in trust risks disrupting the global financial community we all benefit from, and the services we have come to take for granted.

We must ensure our approach to governance will enable the development of digital commerce delivering further benefits to society. New approaches and structures for the leadership and management to counter cyber dependent and cyber enabled crime and subversive activity are required now.

www.ukfinance.org.uk
UK Finance
1 Angel Court
London, EC2R 7HJ
United Kingdom