Cybercrime FCA Paper

A: Current reality: what is happening in this field?
B: Stresses and strains: what are the pressures on the current reality and from where?
C: What could influence the future and how could this play out?
D: Assumptions: Which broadly held assumptions is challenged by this paper.

Introduction

We are living through a revolution. The Internet continues to radically change nearly every aspect of people's lives and has brought untold benefits, but it has also enabled an equally disruptive security revolution to follow in its wake. The advent of the Internet has revolutionised theft, espionage and sabotage for an entire generation. Cyberspace is an ecosystem that has provided the perfect environment for malicious intent. In the UK, the first official estimate of the true scale of cybercrime was recently published and stated that one in ten people in the country had been the victim of a type of cybercrime in the past year alone.[1] 5.8 million incidents of cybercrime were recorded in 2015-2016, including 3.8 million fraud offences and 2.5 million bank and credit card frauds, accounting for nearly fifty percent of all recorded crime in the UK.[2] Despite these figures most experts agree that cybercrime is still underreported. Quite simply we could be living through the greatest crime spree in history.

This new criminal reality has quickly emerged and it is not an issue confined to any one sector, institution or geography. In the space of a decade, Cyber Security transformed from a niche issue to a tier-one National Security problem faced by every major technically advanced state in the world.[3] George Osbourne, in October 2015, symbolically at GCHQ, tripled the National Cyber Security Programme budget first established in 2010 when Cybersecurity was first elevated to one of the four highest priorities in the National Security Strategic Defence review. [4] [5] While often media and governments' focus can be on the strategic end of the debate, financial motivated cybercrime and the consequent impact on businesses is the security elephant in the room.

Unlike traditional National Security threats, industry and the financial sector is the principal target and consequently are shouldering much of the response. In the past decade cybersecurity spending has rocketed and is expected to continue to be a dominant business cost. Government investment is dwarfed by industry seeking to protect itself with predictions of IT Security spending set to reach $101 in 2018 and $170 billion in 2020.[6] The purpose of this paper is to shed light through the optics of a financial institution and financial crime on the current cybercrime reality, the trends and pressures within the field.

Argument

The central argument is that financial cybercrime development in the next five to ten years will be defined by the on-going failure of the community to have discernible and strategic impact against the crime type. Pockets of excellence will emerge, from a public-private partnership perspective, as well as new models of security and capability. However, the fundamentals of the new cyber agenda, the low-cost reward model of the crime-type, the scale of targeting and an ever-increasing global attack surface will mean that only those that invest the most will find any solace in the cyber agenda in the medium-term.

Current reality: What is happening in this field?

The major financial institutions continue to be one of the principal targets of cybercrime, and this is drawing in huge amounts of investment and regulatory pressure at a time of significant change across the industry. Large UK, US and European financial institutions remain at the centre of a multi-layered threat landscape enabled by a

[1] Alan Travis, Cybercrime Figures prompt police call for awareness campaign, The Guardian, 21 July 2016
[2] Office of National Statistics: Crime in England and Wales: year ending March 2016, published 21 July 2016
[3] Jellenc, Eli (2012), Explaining the Global Cyber Arms Race: Strategic Rivalry and the Securization of Cyberspace among Nation States.
[4] George Osbourne, Chancellor's speech to GCHQ on CyberSecurity, 17 November 2015
[5] The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world
[6] "Cyber Security by solution (IAM, Encryption, DLP, Risk and Compliance Management, IDS/IPS, UTM< Firewall, Antivirus/Antimalware, SIEM, Disaster Recovery, DDOS Mitigation, Web Filtering and Security Services)", Global Forecast to 2020, Markets and Markets

low-risk-high-reward model. However, there is no one singular monolithic threat or methodology, rather each cybercriminal, has their own motivations, capabilities, infrastructure and are operating in a competitive and thriving underground economy.[7] This underground economy, hosted on the deep and dark web, is borderless, faceless and has developed a highly efficient crime-ware-as-a-service model.[8] Criminals operate in this realm in almost total anonymity. This space is organised and rewards the deployment of expertise across a range of technical and non-technical services much like any legitimate economy. It is also highly lucrative and is estimated to be costing the global economy $445 billion dollars in 2016, more than the market capitalisation of Microsoft. [9]

How is the industry reacting to this current reality:

- Adopting a holistic approach to security: in order to deliver financial services, institutions have to enable security amongst its customers. The delivery of those services now takes place almost exclusively within the cyber domain and this is requiring institutions to put security at the heart of their organisation at board, operational and service delivery level.

- Technology: the scale and pace of the threat is requiring institutions to invest heavily in next generation technology, including bio-metrics, artificial intelligence and big data analytics for prevention, detection and protection of both their internal assets and customer-facing channels.

- People: in the digital age, it is still the case that humans remain the critical element of defence. This is requiring significant investment in staff as well as customer outreach and awareness of the cyber security threat, including catering to shifting demographics of clients. Efforts to promote cyber security hygiene are falling on a relatively small number of larger institutions.

- Process: in order for technology, skills and investment to protect financial institutions an agile and lean culture must exist in order to match the pace of the ever-changing threat landscape.

What top level causes need to be addressed:

- The Skills Gap: defending against financially motivated cybercrime rests largely on a new generation of highly sought after technical skills. Having a large enough talent pool available to the community, both in the private and public sector that can match the threat requires a major shift in generating a scalable skills pipeline into the community.

- Domestic and International challenges: major cybercrime is largely international in nature and therefore requires cooperation, coordination and partnerships on a global scale. Aligning the complex reality of the myriad of stakeholders in this space, therefore, presents a unique challenge.

- An Effective Deterrence model: technical advances appear to be largely favouring the attacker over the defender in addition to the law-enforcement community. Enabling an effective deterrence model against the new generation of cybercriminals will require new approaches and capabilities at both a policy and operational level.

The Threat Landscape

As a major financial institution, cybercrime is not a new threat to Barclays. Barclays has been targeted for a number of years across the full-spectrum of cyber tactics. The threat landscape Barclays is facing is increasingly polarised; elite groups have moved to seek fewer but larger fraud opportunities while a plethora of cyber-enabled fraud techniques, some relatively unsophisticated, continues to grow. The threat posed is increasingly overlaid with a number of factors such as the continually lowering technical barrier to entry, drawing in traditional fraud teams and the increasing availability of crimeware.[10]

[7] Trend Micro: Cybercrime and the Deep Web, Published March 01 2016
[8] Bradley Barth, Snack Attack: A Crimeware-As-A-Service menu for Wannabee Hackers, SC Magazine, July 13 2016
[9] World Economic Forum, Global Risks Report 2016
[10] Why Cryptocurrency is a perfect vehicle for crime, Let's Talk Payments, 21 April 2016

These cybercriminal marketplace developments can be categorized into two key trends movements: *Upwards* and *Laterally*.

1. Moving up the value chain with higher value attacks.

Elite Cybercrime teams, seeking better return on investment have moved from retail client targeting, following better authentication technology and online channel monitoring being deployed by heavily targeted financial institutions.

Cybercrime teams, principally Russian and Eastern European, are made up of a relatively low number of force multiplying resources and individuals. Estimated to be less than 100 criminals the attacks methodologies deployed by this level of criminal overtime permeate through the underground economy. [11] Sophisticated data mining techniques combined with long-term persistence on corporate and banking entities, has raised the threat level significantly from these teams. Penetration of financial institutions, targeting internal systems has resulted in an increasing number of high profile and high value frauds. A number of elite teams have shown their ability to monitor systems and modify payments in order to hide transactions in a financial institution's internal payment networks.[12]

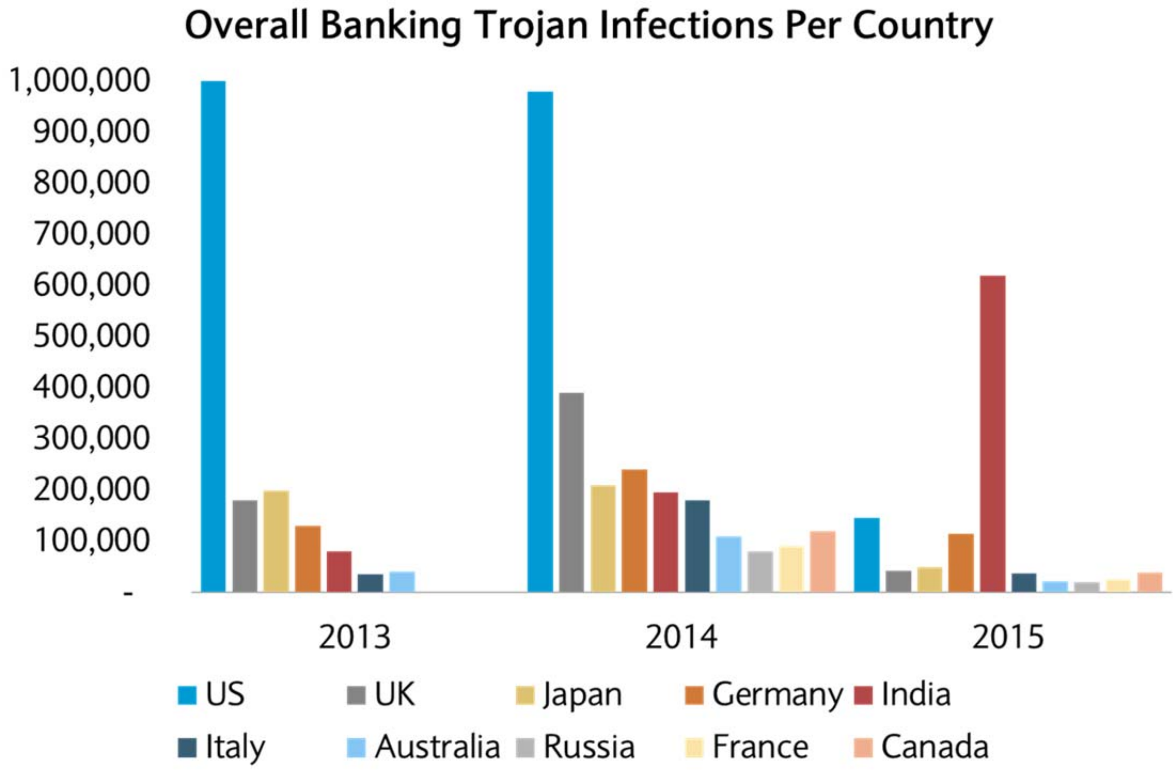
The most recent high profile example of this trend is the recent reports of SWIFT attacks, including the Bank of Bangladesh compromise. This attack highlighted a number of challenges this shift poses across Information Technology, Cyber and Anti-Money Laundering controls. From the publically available information it is clear there are Cyber Security challenges in maintaining a hygiene level that can detect and respond to a full range of attack techniques from readily detectable malware to complex database manipulation and human-behaviour-mimicking components.[13] Similarly, the use of harvested valid credentials poses significant issues for traditional protection.[14] Attacks are at a service and application level and as such protection needs to be service focused as well.

These attacks are not solely determined on a technical or cyber level though, with vulnerabilities in money-laundering procedures and robust cash-out capabilities as important in facilitating attacks. In the case of the Bank of Bangladesh heist the deliberate use of Pilipino casinos , which are specifically exempt from the countries AML laws, should serve as a warning that cybercrime is not a solely Western or technically focused issue.[15] In jurisdictions and institutions where there are issues around cyber security, internal payment controls and anti-money laundering gaps criminals will continue to find fertile ground.

2. Increase in attacks vectors.

Banking malware (a virus specifically configured to hijack a client's online transaction) emerged in the mid-2000s and were designed and deployed largely on a concentrated number of institutions and has been a principal threat vector for a number of years. [16] As a result the most targeted institutions have heavily invested in protection and controls, such as detection platforms based on indicators and abnormalities in technical and human behaviour during a transaction. The resulting concentration and hardening of a relatively small number of institutions has meant that criminals are seeking softer targets in more diverse geographic regions. Available banking malware statistics are indicative of this: [17]

[11] Only 100 Cybercrime brains worldwide says Europol boss, BBC News, 10 October 2014
[12] The Greatest Heist of the century: hackers stole $1 billion, Kaspersky Labs February 16 2015
[13] Christian Beek, Attacks on SWIFT Banking System Benefit From Insider Knowledge, McAfee Labs May 20 2016
[14] Sergei Shevchenko, Two Bytes to $951M, BAE Systems, 25 April 2016
[15] Muhammed Cohen Bangladesh Heist Exposes Laundering Links in Phillipine Casinos, Forbes Asia, 12 April 2016
[16] Trend Micro: A Brief History of Notable Online Banking Trojans, August 31 2015
[17] Symantec, State of Financial Trojans 2013, Symantec, State of Financial Trojans 2014, Symantec, Financial Threats 2015



An overall trend is visible; as those that invest the most harden their defences, criminals move into less protected and experienced countries. This has resulted in cybercrime becoming truly global, with a shift of targeting into European, Asian and the emerging economies. Concurrently cybercriminals are following financial institutions' client base on to new platforms; Kaspersky Labs identified 7,030 new mobile banking Trojans in 2015, and McAfee reported 2.4 million unspecified malware threats in Q4 alone (compared to 1.3 million in Q3), of which more than 20,000 were in the UK.

The fraud losses from these attack vectors are only one element of the cybercrime picture. Banking malware is part of a much wider cybercrime ecosystem that is fuelling much wider fraud. For example, figures from Financial Fraud Action UK indicate there has been a year-on-year increase since 2012 attributed to Internet fraud losses on UK-Issued cards. Over 1.2 million cards were involved in Card Not Present (CNP) fraud in 2015 and this number will almost certainly increase when the 2016 figures are published.[18] In addition, there is a wide array of information stealing techniques that are now default components of spyware, which is been deployed on an industrial scale by cybercriminals.

Point-of-Sale (POS) compromises, merchant targeting, data breaches and spyware are delivering vast volumes of stolen personal data into the underground economy that enables secondary and tertiary attacks. According to data available from a Microsoft's Security Intelligence report nearly 15% of all Windows machines in the UK are infected with spyware. In countries like Brazil this climbs to nearly 33%.[19] CNP and other attack vectors such as Business Email Compromise are enabled by a cybercriminal ecosystem underpinned by this data rich underground economy Business Email Compromise alone, has cost business over $2.3 billion in the past three years.[20]

What changes in the evolving external landscape would most radically impact the industries position?

- Significant changes in financially motivated threat actors moving wholly away from attacks associated with financial institutions to only integrated and direct attacks (ransomware).

[18] Financial Fraud Action UK: Fraud The Facts 2016 – The Definitive Overview of Payment Industry Fraud
[19] Micrsoft Intelligence Security Report, SIR Volume 20, July - December 2015
[20] Adrian Bridgwater, Business email compromise (BEC) phishing scams netting billions for criminals.

- Major capability and changes in international law enforcement ability to consistently and actively disrupt cybercrime that has a major discernible and measurable strategic impact.

- A major cultural or business attitude shift on data protection and information security such as the normalisation of data theft and cybercriminal risks.

- Radical shifts in Nation States cyber behaviour or intent such as actively disrupting or aggressively target major financial institutions and associated CNI.

B: Stresses and strains: what are the pressures on the current reality and from where?

Increased risk and key business differential.

Financial institutions, primarily those that invest the most, are displacing attacks to other institutions but also individuals and small-to-medium enterprises. This displaced targeting poses a fundamental shift and challenge to the financial cybercrime status quo and how cyber security is viewed. Banking organisations are investing significant resources in integrating legacy networks and infrastructure, hardening online channels, and dealing with the fallout of a criminal community which has principally targeted the financial sector. Big institutions are finding the resources to invest, pressured by financial losses, customer expectations and regulatory oversight, but this is ultimately displacing the threat in many instances to more aggressive targeting of clients.[21] This is requiring both investment in back office functions for defence purposes, but concurrently also integrating security expertise into client facing roles and core business service offerings.

Concentrated sector and organisational hardening is shifting criminals, ultimately driven by a return-on-investment model, to target new geographies, individual and enterprises who do not have similar levels of protection. Consequently cyber security is becoming a principal business consideration and is demonstrated by the response to increasing ransomware attacks. Ransomware is becoming a ubiquitous security threat, with nearly forty percent of businesses anticipating an attack in the past year.[22] Kaspersky Labs detected over 230 million malicious ransomware attacks last year, principally directed at individuals and businesses across a whole spectrum of platforms. It a high-visible crime where the potential cost falls directly on the victim and is one of the many pressures challenging the misconception that financial cybercrime is a victimless crime with limited risk for clients.

Fragmented Public-Private response:

The balance and role of public and private bodies in cybercrime is one of the most complex parts of building an effective response to cybercrime. The public and private sectors each face difficult and unique challenges in balancing their varied responsibilities and how best to deploy their resources. However, there are two potential issues to address: *Attribution and Enforcement* in addition to *Regulation and information sharing*:

Attribution and Enforcement

5.8 million incidents of cybercrime were recorded in 2015-2016 but convictions for Computer Misuse Act since 1990 has roughly equated to less than one a month. [23] In July the UK's National Crime Agency (NCA) released its Cyber Crime Assessment 2016, which stated that criminal capability is outpacing Government and Law-Enforcement's response. The NCA suggested that "only by working together across law enforcement and the private sector can we successfully reduce the threat to the UK from cybercrime."[24] Despite heavy investment the law enforcement community appears to be having limited strategic impact on the growth of cybercrime. Without attribution and no fear of prosecution, effective deterrence for financial crime appears to have stalled. While the challenges associated with building an effective cybercrime response are complex, they rest on some fundamental and potentially intractable issues that need to be tackled:

[21] Steve Morgan, Why J.P. Morgan Chase & Co Is Spending A Half Billion Dollars on Cybersecurity, Forbes January 30 2016.
[22] Alex Hern, Ransomware Threat on the Rise as 'Almost 40% of business attacked', The Guardian, 3 August 2016
[23] One computer hacker a month convicted of cyber crime out of 100,000 incidents a year, The Mirror, April 4 2015
[24] NCA Strategic Cyber Industry Group: Cyber Crime Assessment 2016 – Need for a strong law enforcement and business partnership to fight cyber crime.

- An environment defined by a complex and uneven landscape of public, private, and institutional regulations, allowing criminals to easily circumvent law enforcement and international cooperation efforts.
- It requires highly sought after technical skills and capabilities that fall outside of traditional government structures.
- The principle criminals involved in propagating the threat are in hard-to-reach jurisdictions operating behind layers of technical obfuscation, which allows many to operate with near impunity.

Regulation and information sharing

Similarly, the process and public and private sector collaboration in law making, standard setting and regulation is been challenged by the pace of change that defines cybercrime. The creation of standards that can help identify best practices, create shared norms and be constantly raising the security barrier is essential to the cyber-field. Cyber Security ultimately must take lessons from the ‘Black Box’ and open security culture in other industries.[25] The pace of the threat though will continue to far outstrip regulatory authorities’ process for standard setting and consequently a compliance driven security model does not appear to offer adequate protection.

Standards benefit from network effects, but there is a variety of coalitions and institutions that are developing alternative or competing standards. Without critical mass of adoption cybercriminals will continue to exploit gaps in the industries collective defences as has been seen with an uneven patching response that enables a number of point-of-sale attacks.[26] Regulation such as the EU’s General Data Protection Regulation (GDPR) does indicate the powerful potential impact regulation can have. While for some it may carry the implication of a heavy financial burden, it means that by mid-2018, all entities will have adopted a common standard, aligned with how and where they collect, process, and store PII, and required to report any data breach within 72 hours of detection, or face heavy penalties. These two factors could force institutions to significantly enhance data management and security.

C: What could influence the future and how could this play out?

Financially motivated cybercrime is a complex and fast moving arena. As outlined there are clear stresses and strains from a multitude of areas which appear to have a disproportionate impact such as the recent Lurk arrests in Russia. [27] Even if there was increased enforcement capability the fundamentals of the crime type do mean that attacks will continue to rise. Consequently, alternative defence postures must be explored. The following are four technical development areas that could shape the field significantly from a security perspective:

Authentication and privacy: In order to protect financial channels the role of enhanced authentication methodology will be critical. Biometrics including voice and vein technology are already been rolled out by a number of institutions. Fundamentally the next generation of authentication technology, will be based on ever more collection and storage of personal data of their customers, from biometric to live-geolocation data. The Snowden revelations and the ensuing debate indicated that will need to be an acceptable balance between privacy and security and large institutions acquiring, storing and mining data associated with their clients.[28] This debate clearly matters in deploying next generation technology in the fight against cybercrime.

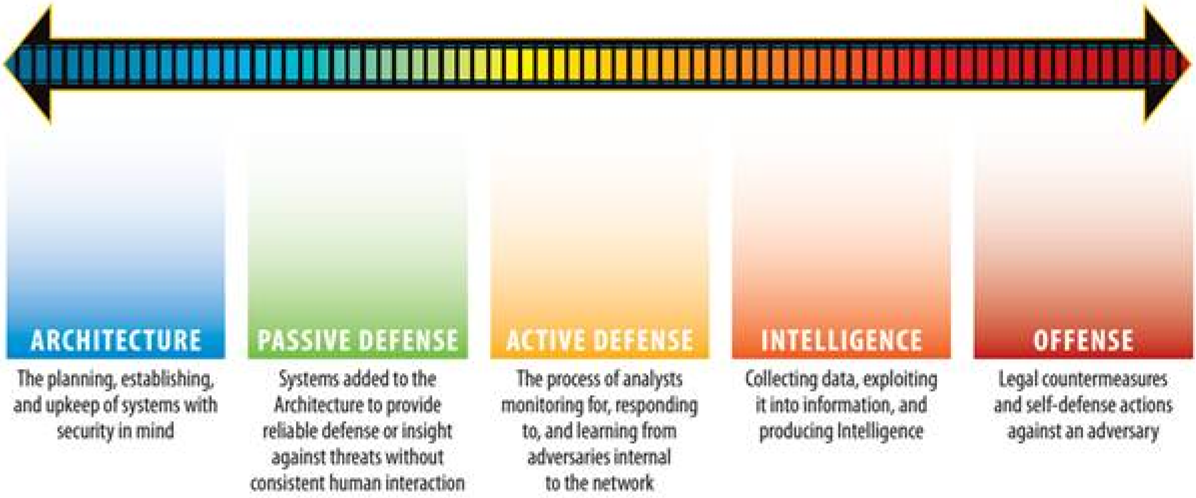
Big Data and Elastic Search: Collection of more data will not be enough. The foundation for effective next generation detection lies in collection, normalisation and enrichment of structured and unstructured data sources. Technology and institutions that can prepare these new data lakes for analysis and create an agile environment will need to transform fraud detection from a factory model to a response based on testing ideas, innovation and analytical skills. Elastic search and other big data solutions are emerging to help create potentially game-changing fraud detection systems and much of it is open source technology. **However, technology can only go so far**; skills, deep expertise and the willingness to manage whole-scale analytical and process changes in institutions are not an insignificant barrier. How the institutions embrace new thinking, manage talent and fully exploit new technology is a significant challenge that will need to be addressed.

[25] Matthew Syed, How Black Black Box Thinking Can Prevent Avoidable Medical Records, Wired
[26] Zach Walker, ‘BackOff’ Point-Of-Sale Malware: What You Need to Know, Rippleshot, 14 September 2016
[27] Kevin Townsend, Did Angler Exploit Kit Die With Russian Lurk Arrests, Security Week
[28] Bob Hodges, Banks Stay Out of the Privacy Debate At Their Own Peril, American Banker, June 15 2016

Security-as-a-Service: One of the key components of cybercrime is the crimeware-as-a-service model. The modular and service-based cybercrime economy has been a key element in democratising cybercrime. Crime-as-a-service (CaaS) offerings have lowered the barrier to entry and it is, not surprising that that the cyber security sector has followed through and developed its own cost-cutting equivalent, giving rise to security-as-a-service (SECaaS). Similarly to its criminal counterparts, SECaaS rests on outsourcing security operations to third-party providers of Internet-based or cloud-based solutions. A move towards SECaaS as a response to the evolving cyber threats is one of the likely developments in the next five to ten years and one that offers a lifeline to small-to-medium enterprises that will increasingly be targeted.[29]

Complete virtualisation of security services ensures the highest degree of capacity and resource utilisation. This makes the service highly cost-effective to the customer and enables pay-per-use models. This not only facilitates the instant commencement of service use, but also leverages inherent data aggregation benefits for service providers. [30] However, SECaaD experience of DDOS does indicate the potential treadmill impact as a service offering. The large uptake DDOS mitigation providers are clearly having an impact in protecting institutions, but ultimately it is not wholly dealing with the threat. Volumetric attacks are becoming more powerful across the landscape and there is a significant rise in application level attacks, a direct result of criminals wanting to disrupt defences offered by mitigation providers.[31] Critical mass of security, scale and a wide defensive posture enabled by these technologies does offer a potential counter-balance to cybercrime, but will need to match the pace and the potential race to the bottom against criminals.

Enhanced offensive capabilities: There is a debate within the cybersecurity community taking a more aggressive or active defence against cyberattacks. The issues surrounding reinforcing cyber defence with countermeasures such as deploying honey badgers, or perhaps most controversially 'hacking back', will crystallise in the upcoming years.[32] However, while there are not only significant legal hurdles to overcome to become part of a sustained commercial response, active or offensive cyber-defence, is at the fully mature end of the security spectrum. Realistically, despite innovations in security-as-a-service offering many companies will not have the investment or inclination to move past architecture or passive defence in the sliding scale of security defence. [33] All but the most mature financial institutions would even be in a position, along with well-resourced Government Agencies, to move into more offensive space and will be dependent on the expertise of commercial providers. In this reality, offensive cyber defence will play no strategic impact in financial cybercrime for the foreseeable future unless SECaaD radically alters the economies and scale of cyber security.


ARCHITECTURE
The planning, establishing, and upkeep of systems with security in mind
PASSIVE DEFENSE
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction
ACTIVE DEFENSE
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network
INTELLIGENCE
Collecting data, exploiting it into information, and producing Intelligence
OFFENSE
Legal countermeasures and self-defense actions against an adversary

[29] Amit Nath, How Security as a Service is changing Cyber Security, Tech2, 11 July 2016
[30] Alison DeNisco, Why Threat Hunting As A Service Is Worth Considering But Not a Silver Bullet, Tech Republic, 1 August 2016
[31] DDOS Attack Activity Rises to Record Level, Q1 State of The Internet, Akamai
[32] Hannah Kuchler, Cyber Insecurity:Hacking Back, Financial Times, July 27 2015
[33] Robert Lee, The Sliding Scale of Cyber Security, Sans Institute, August 2015

D: Assumptions: Which broadly held assumptions are challenged by this paper.

Taking these themes and influences into consideration a **pessimistic** view of the next five to ten years linked to financial cybercrime can be drawn out. The picture of cybercrime is not as bleak as this paper outlines, however only for those that invest in becoming a hard target in the cybercrime landscape. The cybercrime tools, techniques and processes will continue to develop, but their impact can be limited by investment in skills, technology and process that can match the pace of the underground economy. The following are the key assumptions on which the paper's conclusion is based:

- Despite pockets of excellence of next generation sharing and cooperation between law enforcement and industry, an **assumption can be made that the judicial and enforcement response** in the major economies **will continue to falter**. Despite significant government investment, ongoing intractable issues such as having the correct legal and policy frameworks will not keep pace with the technical and criminal innovations of the cybercrime community. Deterrence will continue to be fractured, more attacks across a widening attack surface and more criminals continuing to be drawn into the marketplace.

- Despite innovation in the security industry the fundamental truth, that those that invest the most will drive criminals to softer targets will not change. **An assumption can be that the democratisation of security products, whether SECaaS or innovations in fraud detection, will not be sufficiently radical or universal enough to alter the return-on-investment model of the underground economy.** Criminals will continue to innovate and operate in the margins of error between financial institutions.
- Subsequently, there can be a **challenge to the assumption that financial crime enabled by cyber will exponentially grow for an institution;** it may be curtailed in certain instances, but only for a small number of the most resourced, adept and innovative institutions that can fully embrace technological and cultural change. At a macro-level however, losses will continue to grow year-on-year, especially relating to CNP fraud.
- Further this **challenges the assumption the financial institutions will remain the principal victim of cybercrime;** individuals and small-to-medium enterprises will increasingly become more directly impacted and visibly targeted.