Gadhia
Consultants

The UK's Response to Cyber Fraud: The role of business

IN PARTNERSHIP WITH
HUNTSWOOD

'Economic crime teams need to now be multiskilled functions that incorporate your Fraud and AML investigators, cyber analysts and KYC experts into a single non siloed function under one leadership that uses all the available technology and controls together in a focussed single way to deliver a secure safe environment'

Martin Wilson, MLRO & Head of Financial Crime, Paragon Bank PLC

Introduction

In 2019, working with the Royal United Services Institute, we initiated the research that went on to become the paper entitled 'The UK's Response to Cyber Fraud - A Strategic Vision' authored by RUSI analysts Sneha Dawda, Ardi Janjeva and Anton Moiseienko. At the time, we were aware that the UK's next national cyber security strategy was in the process of being formulated for publication in 2021. Whilst our work with clients showed just how seriously they took their responsibility to protect customers and the significant progress made against fraud in some sectors, what we were not seeing was the acknowledgment or sharing of good practice across different sectors or an awareness of the specific challenges cyber fraud now poses to all UK businesses.

We were determined that the voice of UK business and its' fight against cyber-fraud should be heard and help to influence the 2021 National Cyber Security Strategy. For the first time, supported by Huntswood, we were able to bring together experts from across the counter fraud community to inform the RUSI research. We wanted to hear from representatives from law enforcement, business, NGOs and the cyber security industry to understand what they were experiencing first-hand and what they wanted in the UK's National Cyber Security Strategy.

Amongst the many findings the research identified the prevalence of fraud as the crime type that today impacts every citizen in the UK and that, in almost all cases, fraud was enabled by the internet. The paper called for greater government accountability and highlighted the importance of a 'whole of society' approach to combating cyber fraud. The aim of the research was to develop a holistic set of recommendations to reduce the impact of cyber fraud on the UK. Our approach was to align and coordinate the separate aspects of the 'whole of society approach' with recommendations that connect the counter cyber fraud ecosystem into a more united and strategic approach.

The research identified how criminals have industrialized cyber fraud and highlighted the urgent need for a more strategic and coordinated UK response to combat this growing problem. Based on the research, the paper recognised the importance of a single coherent strategy, led by the Home Office, to combat cyber fraud. It went on to identify 11 complementary recommendations for business, law enforcement and policy makers covering technical takedowns, the need for consistent measurement and KPIs; intelligence and information sharing; increasing public and private sector cooperation and wider support for victims.

The research was categorical in its message that fraud is not a victimless crime, it damages and destroys lives, undermines communities and harms UK prosperity. The National Audit Office expect losses from the Government's COVID-19 loan scheme to reach £26 billion (1) ; everyday, headlines report the growing scale of cyber fraud. Indeed, the UK budget announced a scheme to recruit more than 1,200 new HMRC investigators to combat Covid-19 support related fraud (2) . A survey from across the sector identified the importance of protecting customers and vulnerable people as being central to tackling cyber fraud (3).

This paper builds upon the significant body of evidence that informed the research and extends it to share our reflections as practitioners. The paper also highlights the latest projects already implementing some of the report's original recommendations and how these projects are slowly starting to change the narrative around Cyber Fraud in a more positive fashion.

In this paper we identify three clear, pragmatic actions for business to change the narrative about how we can combat cyber fraud; to reorganise internally to align operations to fight the shifting profile of cyber fraud and to work closer with law enforcement. It is very much the intention of this white paper to help make businesses safer from cyber fraudsters and contribute to making the UK a safer business environment.

Three actions for business leaders

1. Change the narrative

Recognise common challenges, share and celebrate success and demonstrate how, by working together, we can start to win the fight against cyber fraudsters.

In the time that it takes you to read this paper (let's say 30m, UK fraud losses are estimated to have increased by £10.8m; the private sector by an additional £8m and individuals will have lost £0.5m (4). To put this in perspective the estimated losses from fraud are almost equal to the cost of running the NHS throughout the global pandemic (5). The National Crime Agency (6) estimate that fewer than 20% of incidents of fraud are actually reported, which means when scaled up, in the same 30 minutes there were 1,255 (7) incidents of fraud or 41 frauds committed every minute (8).

In a snapshot view of today's news, using the search term 'UK cyber fraud', the top ten organic searches revealed ten headlines about cyber-fraud or cyber-security and none of them were about a successful conviction. Social media will exponentially amplify these stories.

There is a real danger that the media leads us to believe that we are losing the fight against cyber-criminals and that there is an inevitability about this crime-type that cannot be defeated. No one involved in the research believed that cyber fraud was inevitable and the analysis highlighted many individual examples of best practice in combating this crime type. What was missing was a way to bring together these individual successes into one coherent and strategic plan, aligning the activities of the whole counter fraud system and industrialising the UK response to fraud.

There is a responsibility on leaders within both the private and public sectors to change the current narrative and to demonstrate how we are combating cyber- fraud and can start winning against the criminals. We believe that the the time for keeping success quiet for fear of making a business a target is over.

Business leaders need to work with policing, relevant NGOs and with government departments to look for examples of cooperative working between all parties in catching cyber criminals and fraudsters, as well as taking down technical infrastructure.

Businesses also need to actively look for successful stories in which employees have stopped or prevented a fraud, helped a victim, prosecuted a cyber-criminal or recovered stolen funds. Business and law enforcement must not be shy about harnessing the power of social media to highlight success and share best practice. A simple first step is to connect those involved in fighting cyber fraud by joining us in using a consistent social media hashtag #combatcyberfraud which we have identified as a way to help facilitate the sharing and celebration of success and best practice. This new hashtag should become a simple and effective way to connect disparate campaigns and activities; to share best practice; tell and retell success stories and start to change the narrative about how we are winning against cyber criminals.


DO
GOOD
THINGS

2.Reorganise internally

Align operations to fight the shifting profile of cyber fraud and stop regarding cyber security, fraud and financial crime as three different sources of risk.

During the research, interviewees, especially in large organisation, identified the siloed nature of the response to cyber fraud (9). Whilst at the same time noting how criminals have rapidly adapted to change and maximised the opportunities that this presents to them. Yet business still predominantly organises itself in discrete fraud, financial crime and cyber silos which are often inflexible and don't communicate, connect or share information.

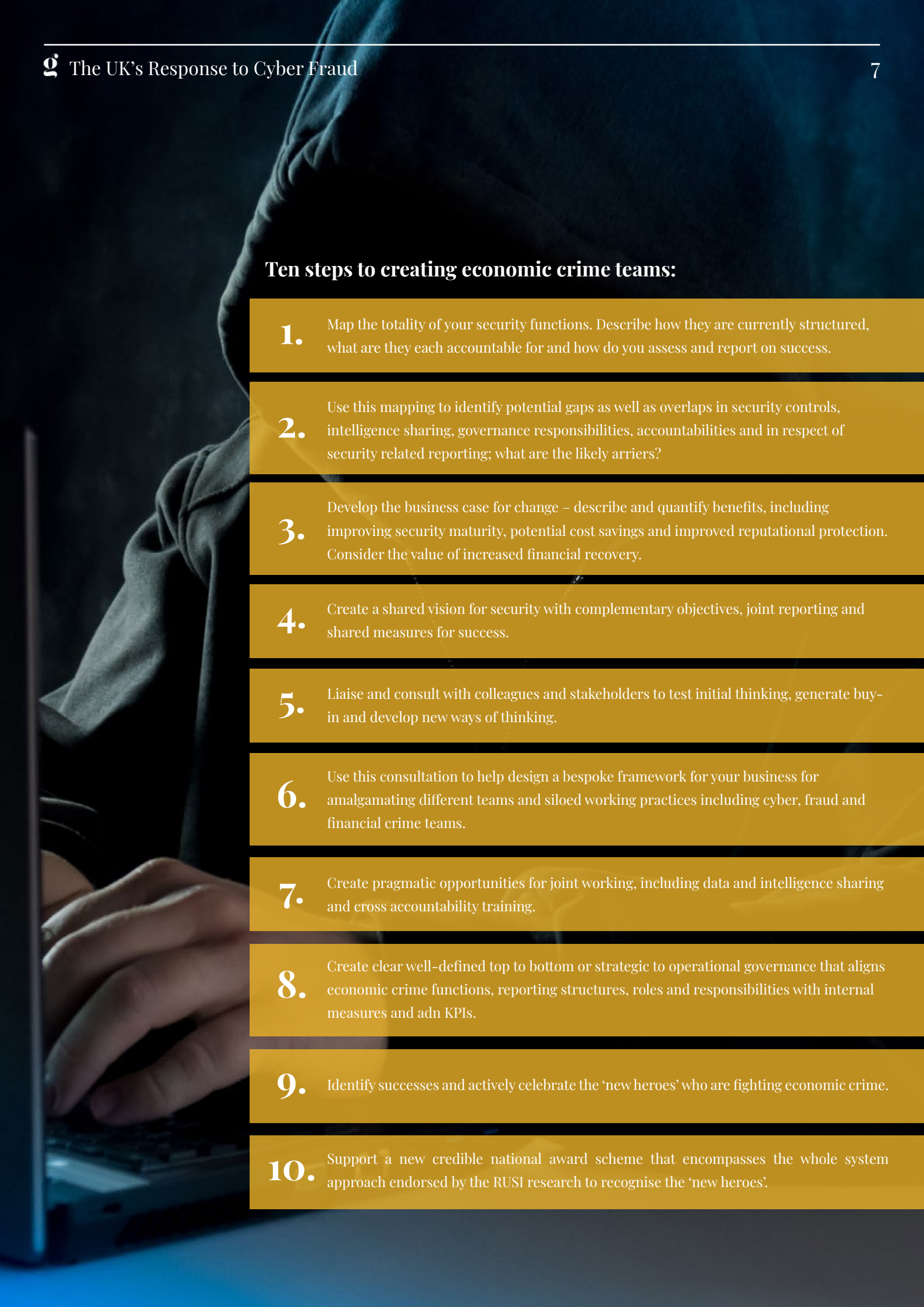
The research did identify some areas of best practice in terms of this holistic approach, but predominantly these were in the public sector where the Home Office and Chief's Police Council recently acknowledged the clear link between Fraud and Cyber Crime by combining the Policing Fraud and Cyber portfolios into one joint portfolio under Commissioner Ian Dyson at the City of London Police.

In business the research highlighted a cultural resistance amongst some practitioners to combining fraud and cyber teams based upon a fear for personal careers rather than any practical support for the more siloed approach.

In our work with clients, we have come across examples of call handlers detecting suspicious or abnormal activity with a customer, whilst the IT function notice a spike in attacks. The two activities in isolation seem insignificant but collectively they are a warning sign.

The vast majority of organisations are passionate about caring for customers, keeping them safe online and protecting the most vulnerable. Criminals on the other hand don't care about customers, want to exploit them online and look for points of greatest vulnerability and in the future are likely to combine more sophisticated challenges through multiple routes. Historically businesses have been functionally organised with IT, cyber security, fraud and financial crime, AML, risk and compliance under different leadership and with different KPIs. Criminals don't think in functions or organise themselves in silos.

Our research is clear that as an organisation's security capability matures there is a strong business case for bringing together all of those involved in defending the business and countering fraud into an integrated economic crime unit. As well as making the business safer from cyber fraud this amalgamation of the different security silos has the benefit of removing potential duplication and decreasing costs; without compromising the importance of governance risk and compliance.



Ten steps to creating economic crime teams:

1. Map the totality of your security functions. Describe how they are currently structured, what are they each accountable for and how do you assess and report on success.

2. Use this mapping to identify potential gaps as well as overlaps in security controls, intelligence sharing, governance responsibilities, accountabilities and in respect of security related reporting; what are the likely arriers?

3. Develop the business case for change – describe and quantify benefits, including improving security maturity, potential cost savings and improved reputational protection. Consider the value of increased financial recovery.

4. Create a shared vision for security with complementary objectives, joint reporting and shared measures for success.

5. Liaise and consult with colleagues and stakeholders to test initial thinking, generate buy-in and develop new ways of thinking.

6. Use this consultation to help design a bespoke framework for your business for amalgamating different teams and siloed working practices including cyber, fraud and financial crime teams.

7. Create pragmatic opportunities for joint working, including data and intelligence sharing and cross accountability training.

8. Create clear well-defined top to bottom or strategic to operational governance that aligns economic crime functions, reporting structures, roles and responsibilities with internal measures and adn KPIs.

9. Identify successes and actively celebrate the 'new heroes' who are fighting economic crime.

10. Support a new credible national award scheme that encompasses the whole system approach endorsed by the RUSI research to recognise the 'new heroes'.

3. Work closer with Law Enforcement

Work more closely with law enforcement to support the prosecution of cyber criminals, improve cyber fraud investigative standards and improve opportunities for inancial recovery.

During the research several commercial sector interviewees suggested a lack of appetite from law enforcement to pursue fraud cases and an associated lack of confidence in achieving successful prosecutions or the recovery of funds. This was often due to the perpetrator being outside the UK or the relative sums being small. At the same time, it was noted by law enforcement interviewees that they were under resourced and lacked capacity to investigate every fraud, despite being committed to pursuing and prosecuting criminals.

We identified a conundrum in the relationship between law enforcement and commercial organisations; in which one side has the capability, capacity and willingness to pursue; whilst the other have the willingness but insufficient capacity and capability. One interviewee from a large financial institution noted 'we operate in the very jurisdictions in which the perpetrators are based and have the means to pursue and want to help law enforcement and yet are never asked'. Whilst there were perceived legal barriers to sharing data and intelligence, more importantly we identified a cultural gap between law enforcement and the commercial sector; this gap often manifests itself as different and sometimes even conflicting priorities, language and working patterns.

Whilst the report makes recommendations for the NCA and ICO to establish the legal framework for information sharing (10) we believe this does not need to be a pre-requisite to a closer working relationship between the public and private sector.

The report does however acknowledge and commend the ongoing work of the information regulators, the ICO and the Global Cyber Alliance, a not for profit amalgamation of public and private sector cyber and fraud professionals who have come together with a new joint project to help create just such an information sharing framework for both the public and private sector and supported by the regulator.

These sorts of practical partnerships were highlighted within the research as a key way for businesses and the police to pursue and prosecute cyber criminals more effectively to the benefit of everyone. However we also found that most private sector organisations were unable to identify their local law enforcement lead for cyber fraud. As a first step we would recommend identifying and building a relationship with either an appropriate local police liaison or with the national specialist cyber and fraud police teams. Beyond that we believe that there is a need to increase private sector capability to investigate and gather evidence in support of cyber fraud prosecutions. If done jointly with law enforcement this will go some way to solving the unequal distribution of capability and capacity between the public and private sector and increase prosecutions and recovery of funds, it will also contribute to the ultimate mission of making the UK a safer environment for all businesses. The report goes on to identify the need for specialist cyber fraud investigator training 'building a cohort of investigators who are equipped to understand the complex nature of cyber fraud' (11). Current training provision tends to be variable in scope, content and quality and we would urge organisations to use accredited or endorsed training providers.

We believe that increasing private sector capability to investigate cyber fraud and making it easier for law enforcement to prosecute will drive a virtuous circle in which more funds are recovered, prosecutions increase and therefore serve as a dis-incentive to criminals.

Again this report can point to exciting new projects involving the Information regulators, the ICO working with members of the Global Cyber Alliance to explore practical options for sharing key data to help partners industralise identifying and taking down criminal sites.

We propose a number of steps to increasing public, private joint working and increasing cyber investigation capabilities:

1. Identify and build a relationship with your law en- force- ment lead for fraud. Developing effective working re- lationships during times of stability mean that these relationships are available for mutual support in times of crisis. Many interviewees stressed the operational and long term business benefit of understanding how to interact with policing at the right level and with the right language.

2. Agree your organisation's appetite for pursue, prosecute and recovery. It was a common theme throughout the research that the adoption of a consistent and successful approach to vigorously pursuing and prosecuting those who seek to attack and steal from us in this way, along with strenuously pursuing the recovery of stolen monies will act as an effective deterrent to criminals. Protecting the business and preventing future criminality. It is important for the Board to engage and endorse this approach.

3. The research clearly demonstrates the need for a counter fraud and financial crime policy that reflects the modern nature of cyber-fraud and the scale of this online crime. There are clear benefits from aligning businesses counter fraud and cyber crime policies in a similar fashion to the creation of joint economic crime teams that reflect the combined nature of the threat.

4. Quantify the value of losses and potential losses including 'near misses' to the businesses from cyber fraud to help build the business case for a risk-based and cost-effective training programme.

5. Implement a formal cyber skills investigation training needs analysis. This will allow organisations to create training programmes specific to their security needs. It provides a framework that helps them identify the needs of individuals, teams and functions and allows them to prioritise training based upon these need and perceived risk.

6. Agree your bespoke approach to pursue, prosecute and recover – selecting to adopt either an in-sourcing or out-sourced approach or as is most common in the businesses we work with, using a hybrid approach based upon risk and cost.

7. As businesses design these training programmes our re-search recommends you use accredited or endorsed pro-viders to implement your bespoke training programme. Our research supported the recommendation for the City of London Police Economic Crime Academy (12) to work with trusted stakeholders to define and accredit national stand-ards of investigative training.

8. Use your training programme to enhance investigation practices and develop new ways of working in line with your pursue, prosecute and recover strategy.

9. Define quantifiable successes measures and set targets for the business in areas of pursue, prosecute and recover. Include regular reporting of these areas at an operational level and through to the Board and responsible executives.

10. Share examples of success amongst colleagues and stakeholders and promulgate examples of best practice amongst peers using a unique # tag.

#combatcyberfraud

Conclusion

Fraud is the crime we are most likely to encounter on a daily basis; it is the crime we are most likely to suffer i n our own homes; it has a widespread effect on individuals, families and communities. RUSI's research in this area has identified this as a national security threat and one that undermines trust in the internet and the government's ability to keep UK citizens safe online as well as impacting UK prosperity.

Our research with RUSI has reinforced the need for a 'whole of society' approach. The paper 'The UK's Response to Cyber Fraud – A Strategic Vision' identified 11 strategic recommendations for policymaker's and key stakeholders and we are delighted to see the practical evidence of the significant progress already being made in respect of many of these recommendations . This paper goes on to identify three practical actions that business can undertake to combat cyber fraud.

We need to change the way in which we talk about cyber fraud, Bob Wigley, Chair of UK Finance has underlined the need to think about it as 'cyber burglary' and as a crime that has direct impact on lives (13). We believe that individuals and organisations can take a small step to change the narrative by consistently using the social media term #combatcyberfraud to share and celebrate success and show how we are winning the fight against cyber criminals. The sum of these small steps should be a powerful combined front against cyber fraudsters.

A more substantive step, that demands imagination and courage, is to align existing departments and functions of cyber security, fraud and financial crime, AML, Risk and all those involved in fighting fraud under a single joint leadership. Behind every attempted cyber fraud is not a teenager in a darkened bedroom trying to make some money but a sophisticated network of organised criminal groups, including sometimes state actors using the latest technology and brightest brains to exploit vulnerabilities in cyber defences and human nature. Organisations run the risk of being trapped in a cycle of being at the limit of their capacity fighting cyber- crime and, therefore, unable to find the space to think about how to reorganise.

As policy makers develop the framework for a 'whole of society' approach, we believe business should actively take steps to work closer with law enforcement. Our research shows that law enforcement has the appetite but not the capacity to investigate every cyber fraud. By increasing the capability of the private sector to investigate cyber fraud, we will build a better system that has appetite, capability and capacity to prosecute cyber fraudsters and recover stolen funds.

Finally, we believe that we are at a turning point about how we think about digital business. On the 3rd April 1995, Amazon sold its first book online; 26 years later we can buy almost everything online. The global pandemic has accelerated all digital strategies and our lives as we shift to 'online everything'. Today the UK's cyber security industry is worth an estimated £8.3 billion, with revenues in the sector up 46 per cent from £5.7 billion in 2017 (14). There is a risk of assuming that there is a linear relationship between spending on cyber security and being cyber secure – the more you spend the safer you are. It is not by chance that the Greeks outwitted the strong walls of Troy using subterfuge and the Trojan Horse of legend. The defenders of Troy assumed their strong walls were enough and they were outwitted by a sophisticated enemy. Cyber security strengthens the walls but now we have a greater definition of the task as combatting cyber fraud. This is more than semantics; it is reframing how organisations think about the purpose of cyber security and how the whole of society organises itself to defeat fraud.

The authors

Stephen Head MA, FRSA
Senior Partner

Stephen was formerly Chief Security Officer at Virgin Money where he developed a forward looking holistic approach to security and to the overall operational resilience of the whole business.

As a former Commander at the City of London Police he was the first National Coordinator for Economic Crime, responsible for leading and coordinating the national policing response to economic crime including cyber-enabled crimes, fraud and Anti-Money Laundering.

He has worked internationally advising ministers, senior policing officials and other law enforcement agencies about national and international counter fraud and cybercrime strategies. He has worked across the private and public sectors to raise awareness of the growing threat of Cybercrime and the importance of integrated security defences with effective Board oversight.

Stephen is a graduate of the FBI's National Academy and has an MA in Criminology from Cambridge University. He is also a Freeman of the City of London and a member of the Security Professionals Livery Company.

Mike Peckham MA, FRGS, FRSA
Managing Partner

Mike has provided consultancy support and specialist advice to a range of blue chip clients including De Beers Diamonds, Starbucks, BSB Sky, EDF, Total Exploration and Production, Tullow Oil, North Caspian Operating Company (Kazakhstan) and Virgin Money. As an operations specialist he has managed special projects for Virgin, De Beers and Total in West Africa, sub-Saharan Africa and Yemen.

Mike is also a non-executive director of the Airbox, providing mission support, location tracking and control to UKSF, UK Armed Forces, Emergency Services and Policing. He is non-executive director of the Lumus360 ™ an organisation that specialises in providing online 360 degree feedback and psychometrics.

Beyond work he is a Trustee of the Armed Forces charity Hire a Hero; Chair of the trauma recovery charity SAFE; He is a Visiting Fellow at the Business School of the University of South Wales and lectures at the MoD's Defence Academy, Shrivenham.

About Gadhia Consultants

Established by Dame Jayne-Anne Gadhia in 2019, Gadhia Consultants work with policy makers, law enforcement and the public, private and third sector to improve how they fight cyber fraud, economic crime and improve cyber security

We are an experienced team of cyber security, fraud and financial crime and security professionals that bring that expertise to board level education and review, audit and advise you how to better fight economic crime.

Whilst there are many questions for senior executives, we believe there is a critical question:

'How can I independently verify that my organisation is safe from the risk of economic crime'

In other words, how can I be sure I am doing the right things to keep customers, colleagues and the organisation safe as the threat landscape changes?

Gadhia Consultants work with organisations to review, audit and advise in the following areas:

- Fraud and financial crime strategy and governance
- Cyber security strategy and governance
- Combatting fraud and economic crime
- Organisational design, training and development for joint team working
- Cyber resilience
- Emergency response and operational resilience
- AML, KYC and DD
- Training in cyber investigation skills

About Huntswood

We are Huntswood. The people who put partnership first. A trusted team with the insight, expertise, and pace to create better outcomes for our clients, their customers, and the communities they are a part of.

We deliver resourcing, outsourcing and advisory services from complaints to customer service, remediation to resilience – bringing together the people, processes and knowledge businesses need to succeed.

We're built on the ambition to make a positive difference. It's what Huntswood has done since we opened our doors 25 years ago, and it's what every single one of us strives for today. Over the years, we've grown from a two-person team to a nationwide service provider – accepting bigger challenges, exceeding clients' expectations and empowering each other every day.

We put the right people in the right place at the right time – whether it's our dedicated team of Associates or our Board. Together, we've got the outstanding track record of delivery, the depth of expertise and the flexibility of approach to be the trusted partner our clients deserve.

We stand with our clients without question, working on their terms to share our insight whenever and wherever they need it. The pressure for businesses to deliver higher quality services at lower costs is growing. Firms are reinventing how they operate, execute and communicate – adapting to new ways of working and responding to changing customer needs in different ways. We're here to help clients as the landscape evolves and new challenges arise. We advise and consult as a trusted partner in times of change – offering ultimate flexibility to help clients create value and meet demand with confidence.

We deliver insight for better outcomes, and that means being there to help clients navigate change, invest in the future and meet challenges head-on. It means helping them anticipate what's next and solving problems before they even arise – with minimum risk every step of the way.

We are Huntswood. Your trusted partner for better outcomes.

Referrences and accreditations

1. https://www.nao.org.uk/press-release/investigation-into-the-bounce-back-loan-scheme/
2. https://citywire.co.uk/wealth-manager/news/budget-2021-hmrc-to-recruit-1200-for-tax-clampdown-taskforce/a1475083
3. Dawda, S., Janjeva, A. and Moiseienko, A., (2021) The UK's Response to Cyber Fraud, A Strategic Vision, Occasional Paper, RUSI; London – Page 45
4. This is based on a pro-rata calculation from the report 'Annual Fraud Indicator: Identifying the Cost of Fraud to the UK; that estimates the Annual UK fraud losses to be £190 billion; Public sector fraud losses to be £40.4 billion; Private sector fraud losses to be £140 billion https://www.crowe.com/uk/croweuk/insights/fraud-indicator-report-2017
5. The 2017 Annual Fraud Indicator report estimated losses from fraud to be £190bn; the 2021 NHS Budget is £201.7 bn.
6. https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime
7. ONS, 2020, Crime in England and Wales: year ending September 2020; Estimates from the Telephone-operated Crime Survey for England and Wales (TCSEW) showed that there were 4.4 million fraud offences in the last 12 months.
8. This is supported by Blakeborough, L., and Correia, S.G., (2019), The Scale and Nature of Fraud: A Review of The Evidence'; The Home Office that estimates only 17% of CSEW fraud was reported to the police or Action Fraud. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720772/scale-and-nature-of-fraud-review-of-evidence.pdf
9. Dawda, S., Janjeva, A. and Moiseienko, A., (2021) The UK's Response to Cyber Fraud, A Strategic Vision, Occasional Paper, RUSI; London – Page 53; Footnote 126 - Author interview with a cybercrime specialist at an international organisation, 6 May 2020; author interview with a representative from an information-sharing group, London, 21 July 2020; author interview with an information-sharing platform, 21 July 2020.
10. Dawda, S., Janjeva, A. and Moiseienko, A., (2021) The UK's Response to Cyber Fraud, A Strategic Vision, Occasional Paper, RUSI; London – Page 12; Recommendation 5: The National Crime Agency, in consultation with the Information Commissioners' Office, should publish comprehensive guidance for private sector organisations on how they can lawfully assist law enforcement in preventing and investigating cyber fraud through information sharing.
11. Dawda, S., Janjeva, A. and Moiseienko, A., (2021) The UK's Response to Cyber Fraud, A Strategic Vision, Occasional Paper, RUSI; London – Page P46
12. Dawda, S., Janjeva, A. and Moiseienko, A., (2021) The UK's Response to Cyber Fraud, A Strategic Vision, Occasional Paper, RUSI; London – Page 13; Recommendation 10
13. Bob Wigley – RUSI Panel discussion 1st March 2021.
14. https://www.gov.uk/government/news/uks-booming-cyber-security-sector-worth-83-billion

10 Norwich Street,
London,
United Kingdom,
EC4A 1BD

T: +44 (0)203 983 0933
T: +44 (0)7860 709890
E: mike.peckham@gadhiaconsultants.com

GadhiaConsultants

IN PARTNERSHIP WITH

HUNTSWOOD