Partnering Up Against Cybercrime

27 May 2021

Chaired by **Justin Partridge,** University of Leeds

Session 1: Strategy

Interests in common: Working with the private sector to maximise resources and build partnerships for the future of cybercrime - Brian Dilley, Lloyds Bank

Creating a new win-win: why technology will change policing and private sector objectives - Mandy Haeburn-Little, Business Resilience International Management

Session 2: Practice

'What's it got to do with us?' - A case study in partnering with small businesses to build resilience - Martin Wilson, NEBRC

University and Police Partnership in Cybersecurity**:** How ethical hacking and cybersecurity research are helping small and medium businesses - Dr Biju Issac, University of Northumbria

Report

On Thursday 27 May the event was chaired by Justin Partridge, Postgraduate Researcher at Leeds University Business School and Visiting Fellow at the Open University Centre for Policing Research and Learning, and introduced by Dr Geoff Pearson, Academic Co-Director of N8 PRP.

The programme looked at the strategy and practice of policing business-related cybercrime, drawing on a wide range of experience in fraud prevention, business resilience, and cybersecurity research and policing. All of the speakers are involved with the North East Business Resilience Centre, an innovative non-profit organisation that brings together national financial institutions, academic expertise, and businesses to develop cyber safety for businesses and customers.

Sharing resources

Brian Dilley, Group Director of Fraud and Financial Crime Prevention for Lloyds Banking Group and Chair of NEBRC, began the session with a presentation on the obstacles and opportunities of public-private partnerships in policing cybercrime.

A major obstacle in effectively identifying and responding to suspected criminal activity is data sharing. Brian discussed how this was addressed by two partnerships established by the National Economic Crime Centre (NECC). Firstly, the Joint Money Laundering Intelligence Taskforce (JMLIT) formalises data-sharing arrangements between financial institutions to enable early identification and evidence-gathering of criminal activities. Secondly, the Otello Covid-19 Fusion Cell aims to identify changes in the economic crime threats as well as sharing information. This type of partnership saves police time and resources through pro-active reporting and analysis.

Along with access to data, a significant obstacle in effective partnerships is the disparity of resources available between the public and private sector. Brian looked at how this was addressed firstly, through direct funding of regulatory activity by the private sector through the Dedicated Card and Payment Crime Unit, a dedicated national police unit that is fully sponsored by the cards and banking industries that is estimated to have prevented £20m worth of fraud in 2020. Brian acknowledged there were concerns about the risk of creating a 'private police force' which had been raised during parliamentary questions, but argued the funding was appropriate in this case due to the remit of the unit and the skills required to operate it.

Secondly, Brian discussed the partnership between Lloyds Banking Group and City of London Police, which provides economic crime training for officers, a technical advisory hotline for investigators, and delivers the 'Cyber Detectives' course to schools in England. Resource disparity is therefore mitigated through partnerships which enable the financial sector to directly fund regulation and training.

Brian acknowledged however that these resource-sharing partnerships did not address the disparity in pay between the public and private sector. This disparity is a key concern for public sector managers when considering partnerships with financial institutions, or when even putting staff forward for training. Brian gave the opinion that police should not try to block movement from public to private roles, as this was self-defeating as it reduced the skills and capacity available to police. Brian argued that public employers should instead focus on the benefits they offered as a place of work, especially with regards to the job satisfaction and sense of purpose to be gained from working in policing.

Innovation and sustainability

Mandy Haeburn-Little, CEO of Business Resilience International Management, looked at the current status of the UK tech sector, what this meant for policing and cybercrime, and considered two partnerships that are responding to these changes.

The UK tech sector is the third most valuable in the world, and still growing rapidly. This creates the need for cohesive vision of cyber security across public and private sectors. When UK businesses where surveyed, there was a clear reliance on technology – eg business banking, promotion, holding customer's personal data. However, 25% were running an outdated version of Windows, increasing their vulnerability to cyberattacks. Additionally, there is increasing use of technology in policing, including facial recognition, body worn cameras, thermal imaging and smart cruisers.

In this context, public-private partnership is essential to match police intelligence and specialism can be matched by private sector scale and speed. An excellent example is the Police Cyber Alarm developed by The National Cybercrime Programme (NPCC), which collects data on attempted cyber-attacks and reports on this to both the member organisation targeted by the attack and to cyber-crime units to be analysed at a local, regional, and national level. The vibrancy of the UK tech sector can therefore be harnessed to dramatically increase the capacity of police to understand and respond to cybercrime.

However, to create a cohesive vision sustainable partnerships are required. To achieve this, the UK has created a network of Cyber Resilience Centres to encourage and develop partnerships, assess business needs, innovate solutions, and to share best practice. This network of regional centres is a joint platform for private sector and policing, are they are key to developing a national 'nexus of trust' in partnerships to tackle cybercrime.

Hesitations and Opportunities

In the following Q&A session, the discussion focused on the hesitations of police management to partner with the private sector. Brian talked about the concern managers had of staff using training opportunities and secondments to jump to the private sector, and wanted to encourage managers to see development opportunities for staff as a net positive whereas blocking development could only adversely affect staff satisfaction and police capacity. He also referred to the benefits of working for the police that the private sector simple could not offer, such as the rewarding work of investigation. Mandy added that in the future she would like to see the possibility of roles split part time between a public and private institution.

Concerns over private bodies taking over public roles was also discussed. Brian said that in his experience reassurance that the scope of private influence was appropriate depended on the trust built through interpersonal relationships, which presented a challenge when considering the expansion of partnerships like JMLIT. The importance of these relationships is a key reason why the ambition for JMLIT was to be co-located with police.

On partnership with academia, both Mandy and Brian agreed that this was invaluable. Mandy added that for innovation to work there needed to be room for mistakes, and development structure of academia was vital for this.

Finding what works

The second session began with Martin Wilson's presentation on the North East Business Resilience Centre and their experience of helping SMEs to develop better cybersecurity.

Picking up from Mandy's presentation, Martin discussed the role of the Cyber Resilience Centres. The NEBRC is one of 9 CRCs nationally that work with ethical hacking students to provide businesses with cyber resilience services. This includes vulnerability assessments, security training, and continuity planning. The aim of the model is to provide development opportunities for students as well as building the regional economy through improved business resilience.

However, in order to create effective guidance, Martin argued it is vital to understand and address why many SMEs are slow to adopt cyber security measures. Martin gave an overview of the current literature, which suggests a lack of knowledge by business owners who are put off by an overwhelming amount of available advice, a tendency to underestimate the risk or cyber-attack, mistrust of being 'oversold' by the sector, and a high acceptance of risk, particularly among entrepreneurs. Looking to address this, there has been relatively little work on SMEs, so NEBRC used literature from other fields including health, behavioural economics, and health and safety, to develop an approach that would be accessible and motivating for SMEs, identifying what factors prompt businesses to adopt secure behaviours. These finding were used to create the 'Cyber Security: Small Business Guide' by the National Cyber Security Centre. NEBRC is continuing to develop this work with research on SMEs specifically, and have conducted a survey of 70 SMEs in the North East, and are working with SMEs on trial interventions.

Developing skills

In the final presentation of the day, Dr Biju Issac discussed how the student-led Cyber Clinic partners with NEBRC. There is currently a significant skills shortage in cyber resilience, so it is important to

create development opportunities for students to grow the sector and prepare them for careers, as well as addressing the immediate need of businesses for improved cyber security.
The Cyber Clinic draws on students from Northumbria University's Cybersecurity and Digital programmes which has nearly 300 students. Due to the university's partnership with NEBRC, a programme was developed wherein NEBRC now employs 9 students as part-time cybersecurity consultants, and a further 5 have been appointed. The students create guidance and training for business, for example through infographics and webinars on topics like ransomware and the commodity threat landscape, as well as running services such as web app vulnerability tests. This partnership addresses both the current skills shortage and builds a stronger foundation for the sector for the future.

As well as working with NEBRC, Cyber Clinic students are running projects on using artificial intelligence (AI). Current projects include detection of online hate speech, phishing, data exfiltration, botnets and malware, as well as working directly with police to create an intelligent intrusion detection system. Biju emphasised that the skills and innovation available among students were essential to addressing cyber-crime. Biju concluded that cyber-attacks are too complicated to be dealt with by any one party, and partnerships between government, police, universities and business – as seen with the CRCs – are essential.

Putting innovation to use

In the discussion, Biju talked about the importance of giving students the opportunity to implement their work rather than being satisfied with a paper or presentation, as there is a huge pool of talented work and innovation that goes unused.

Justin wrapped up the session by asking each of the speakers if there was one change they would like to see. Brian responded that there needed to be a much better sense of where the skills were and a focus on maintaining them, which required effective public-private partnership beyond active cases. Mandy commented that connectivity had improved, but she would like to see the development of a grassroots knowledge of the presence and benefits of the cyber centres. Martin said he would like to see partners using the cyber centres as a basis for research, and so generate more ideas and creativity. Biju added that he would like to see more openness to building bridges, so partnership working became the norm so knowledge and experience was not kept within silos.

Speaker Biographies

Martin Wilson, Head of Student Services, NEBRC
Martin Wilson of Durham Constabulary has 16 years policing experience across various policing roles. Prior to joining the NEBRC, Martin was part of the North East Special Operations Unit (NERSOU). He specialised in Cyber Protect, Prevent and Prepare work streams, leading on new and innovative work, helping businesses understand and prepare for cyber-attack. Martin and his cyber teams have been recognised locally, regionally and nationally, winning awards for their crime prevention work. Martin lives in the North East with his wife and young child, and in his spare time enjoys skiing, running and reading.

Brian Dilley, Lloyds Banking Group/Chair of the NEBRC Board
Brian is responsible for fraud prevention, anti-money laundering, sanctions compliance, anti-bribery and countering terrorist financing across all of LBG's brands. Brian holds the Senior Manager Regime position of Money Laundering Reporting Officer for Lloyds and Bank of Scotland.

Brian has held a number of external positions within the industry, among them Chair of the Economic Crime Product & Service Board at UK Finance, member of the JMLIT Management Board & member of the Joint Fraud Taskforce Oversight Board. He also represented the banking industry on the Steering Committee that created the Authorised Push Payment Scam Code in early 2019.

Brian has over 20 years' experience of Fraud & Financial Crime, the vast majority of which has been in financial services. Prior to joining Lloyds Banking Group Brian was the Global Head of Anti-Money Laundering Services and led the UK Financial Services Forensic team in the consultancy practice at KPMG. He spent over four years at the Financial Services Authority where he was Head of Department in the Enforcement Division during the implementation of the Financial Services & Markets Act and the development of the FSA's Financial Crime strategy. Whilst at the FSA, Brian conducted the FATF mutual evaluation of Latvia and was part of the team that responded to the mutual evaluation of the UK.He then spent over three years at UBS Investment Bank where he became Managing Director and Global Head of AML Compliance.

Mandy Haeburn Little, Business Resilience International Management
Before founding BRIM in 2019, Mandy was the Chief Executive of the Scottish Business Resilience Centre for over nine years, working in direct partnership with the single police force, Police Scotland and the Scottish Government. Mandy developed a range of affordable, innovative services for small and medium sized businesses. Working with the Directors of student services at BRIM, a new talent pipeline and BRIM set of business services have been developed which support emerging students of forensics and vocational cyber security whilst also benefiting the business community. Over time, it is intended that these students will go directly into policing and this activity is already developing. This model, as well as engaging business of all sizes in proactively delivering cybercrime prevention advice, has been the cornerstone of the National network that Mandy and her team are delivering.

In Scotland Mandy chaired the Cyber Expert group, the network of trusted security partners, was the only independent Board member of the Scottish Crime Campus and sat on the Serious Organised Crime Force.

On announcing her departure from her role as CEO, Mandy received a cross party commendation from the Scottish Parliament for her outstanding contribution to the business sector as well as for her transformational leadership.

As well as leading and delivering the national Programme of Cyber Centres for Policing, Mandy is also now working directly with National and International business leaders on the creation of a single National entity which will support the network of Regional Cyber Resilience Centres.

In 2020, Mandy received an award from CS European Awards and a Police commendation for her Outstanding Contribution to the Cyber Industry for her work involved with the Scottish Business Resilience Centre and her most recent project in establishing Cyber Resilience Centres across the UK. In January of this year, Mandy was invited on to the first Cyber Expert Panel set in place by the Home Office in order to review the National Cyber strategy.

Biju Issac, Northumbria University/ Advisory Group NEBRC
Dr Biju Issac is the Programme Leader of 'Computer Network & Cybersecurity' and 'Computer & Digital Forensics' courses at Northumbria University with around 300 students. He has done PhD in Networking and Mobile Communications, Master of Computer Applications (MCA) and Bachelor of Engineering (BE) in Electronics and Communication Engineering. He is a Chartered Engineer (CEng), Senior IEEE member and Fellow of HEA. Northumbria University is recognised as an Academic Centre of Excellence in Cyber Security Research (ACE-CSR) by NCSC and EPSRC. He founded 'Northumbria Cyber Clinic' in 2018, where the Cybersecurity and Digital Forensics students are trained in ethical hacking and pen-testing using Kali Linux tools every week to prepare them for the industry.

His research interests are in computer networks, cybersecurity, AI/machine learning applications (in security, text mining, image processing etc.) and technology in education. He is currently involved in cybersecurity and AI/machine learning projects with PhD students under him and his personal research website is https://www.bijuissac.com/.

Justin Partridge, University of Leeds
Justin has worked across the public sector, in Local Government, Civil Service, London Fire Brigade and several police forces. His roles in those organisations have been equally varied, including IT, programme management, running London Fire Brigade's training centre, working with Lincolnshire Police on the outsourcing of services to G4S and establishing collaborative policing for five police forces in the East Midlands.

His most recent employment role was leading a series of collaborations between seven police forces in the north east of England, working directly to all seven Chief Constables and Police and Crime Commissioners. As well as leading this regional programme, he was responsible for understanding national programmes of work and working with the Home Office and others to implement these in the north east. This role builds on previous experience establishing a similar five force collaboration in the East Midlands between 2005 and 2010.

Previously Justin was Director of Corporate Development for Humberside Police, responsible for major change programmes, performance and information compliance amongst others. One key part of his role there was to enhance how the force can use evidence based practice to improve service to the public, working with several universities and forces around the country. Whilst in this role Justin joined both the N8 Policing Research Partnership and the Open University centre for Policing Research and learning, sitting on the steering groups for both of these police academic partnerships. As part of the N8PRP, Justin was instrumental in proposing an innovative series of CPD events for police data specialists, which has been well received across eleven police forces in the north of the country.