techUK

How can the technology community help combat the changing fraud threat?

techUK briefing note | September 2018

techUK is conscious of the challenges facing law enforcement and policy makers in a world where traditional models of recording and investigating crime are proving no match for emerging technologies. Developments in tech have given police forces better tools to combat crime, but technologies can also enable credible threats to be delivered simultaneously to multiple targets at marginal cost by almost invisible adversaries. The victims can be governments, organisations or individuals - but the criminals' tools are largely the same.

With fraud now the most commonly experienced crime in the UK, techUK convened a roundtable discussion bringing together law enforcement, government, industry and the third sector to explore how technology can best be harnessed to combat fraud.

Background

Fraud is the most commonly experienced crime in the UK. The Crime Survey of England and Wales (CSEW) 2018 indicated that there were 3.3 million incidents of fraud over the last year.[1] And over half of all fraud is online. The NCA Strategic Assessment of Serious & Organised Crime published in May 2018, emphasised the importance of fraud, and highlighted that "our understanding of fraud in the UK is hampered by under-reporting; less than 20 per cent of incidents are reported to the police."

At a recent briefing in the City, delegates heard the CEO of a financial institution describe the initial steps that she would take in the event of a cyber fraud attack. The first question is addressed to the CTO: "has it stopped?" The second question is to the Head of Communications: "Is the attack in the public domain – has our reputation been damaged?" and the third question is addressed to the Head of Audit: "Find out what happened - and the extent of the damage done". Some time later, it's likely that someone will ask the question "Should we perhaps contact the police?"

The challenge facing the police and other bodies charged with investigation is how to remain relevant in this arena as the proportion of non-reported incidents continues to grow. As the technological competence of criminals increases, **how can the police ensure they have the right tools and expertise to tackle the threat of fraud?**

Current landscape

Once crime is on the internet, national borders are irrelevant. This contrasts with law enforcement, which in the UK is of course neatly sub-divided by county. When it comes to fraud, blurred boundaries between interested parties (public sector & private) mean that information can easily fall through gaps – under reporting of fraud makes it hard to understand the full scale of the issue.

Fraud is gaining prominence as levels rise. But the capacity and capability of law enforcement to tackle this threat is limited. In spite of increased government focus, this might not translate into additional resources for fraud investigation. If the police do get additional money in the next Spending Review, combating fraud will have to take its place in the queue of other demands. Policing is under acute pressure with 999 and 101 call levels at all-time highs and with safeguarding, major enquiries and other priorities stretching the police (especially detective capability).

Police effectiveness will be helped by the delivery of some national programmes. The Digital Intelligence and Investigation Programme (DII) and National Law Enforcement Data Programme (NLEDP) will facilitate the sharing of data within policing. But there is more to do across agencies.

Traditionally, the police held the intelligence they needed within policing but now - with the increasing complexities of cyber and internet-enabled fraud - much more of the data that policing needs sits outside of its control.

Whatever the outcome of Spending Review, there seems to be substantial benefit to all parties from a more collaborative approach to fraud. There needs to be a new model of closer collaboration and sharing, be it secondments of staff, education or better data sharing.

1. Crime in England and Wales: year ending March 2018: https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingmarch2018

Key issues

The extent of the problem: one organisation revealed that its survey data indicates that 50-60 per cent of businesses are victims of fraud each year.

Geography: the police resourcing problem is compounded by the fact that the investigation often falls to a force simply by virtue of the address of its registered office: the offending may well have taken place in a separate county or country (or multiple areas). For elected representatives of local communities, it is hard to prioritise these crimes with little local impact.

The dispersed nature of victimisation: one participant revealed that 5 per cent of insurance business is tainted by fraud. This cost is shared – largely in ignorance - by the remaining 95 per cent of honest policyholders.

Understanding harm: it is hard to quantify the 'level of harm' caused to both individuals and businesses by fraud. Some work has been done to try and assess this. If a more comprehensive assessment were made, it might help police make the case for more resource and would aid in public education efforts regarding the importance of cyber security.

Under-reporting: the consensus among the group was that there are significant levels of under-reporting of fraud. Three reasons were suggested that might explain under-reporting of fraud: the difficulty in reporting; reputational risk; and the assumption that there will be no satisfactory outcome.

The first of these will hopefully be addressed (to some extent) by the new version of Action Fraud. The issue of reputational risk is an attitude that can in part be overcome by fostering a more collaborative relationship between industry and policing. The third issue, a lack of enforcement, will in part be addressed as policing becomes more digitally capable. But given the calls on police resources and the scale of fraud, prevention more than enforcement is where the major gains lie.

Data sharing: one investigator described the problem of technology systems that are incapable of 'talking to each other'. Sharing data is an operational priority but a combination of factors make it difficult. Some of these relate to interpretation of the legislative framework, but others are technological – the unwillingness of all technology companies to work collaboratively with open APIs, etc.

Lessons could be learned from approaches adopted in other sectors: including a consortium of suppliers and customers in Health & Social Care who have launched "INTEROPen". This is a coalition of the willing to incentivise collaborative behaviours on the part of technology suppliers, and reward it by making contracts more readily available to the most collaborative: in the interests of the citizen.

Identity verification: a key factor in deterring or reducing fraud. Wider uptake of digital identity verification tools could be accelerated by a strong steer from Government and policing, to encourage businesses and individuals to adopt these technologies.

Skills: Police are aware of the cyber and digital skills shortage they face. There is a need to explore more pathways for engagement with the private sector, where many of the skills reside. Two-way secondments, where industry experts are placed in forces, and would see police officers spend time with businesses

understanding how they deal with fraud, should be explored.

Key technologies and proposals

The group identified some key technologies that should be utilised in the fight against fraud:

- Natural language processing;
- Automated entity extracting;
- Automated analytics;
- Open source intelligence analysis.

techUK members will work with police forces to improve their access to and understanding of industry capabilities in these areas.

techUK will pursue the activities in order to address the issues above:

- **Establishing two-way secondments between policing and industry:** to allow industry and policing to share skills, experiences, and expertise.
- **Exploring the viability of setting up a policing equivalent of InterOpen:** to incentivise collaborative behaviour among the tech supplier community.
- **Encouraging adoption of digital identity verification tools:** a crucial tool in fraud prevention.
- **Working to understand the harm caused by fraud:** to increase awareness of the threat.

techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow.

950 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK.

These companies range from leading FTSE 100 companies to new innovative start-ups.

The majority of our members are small and medium sized businesses.

techUK.org | @techUK | #techUK