Policing borders after Brexit - Combatting online identity theft

As Britain prepares to leave the EU, the question of what UK's borders should look like is high on the political, economic and security agenda. The policing of UK borders post-Brexit is further complicated by security concerns of online identity verification of people passing through our ports, underpinned by the rise of increasingly sophisticated attacks by cybercriminals to steal identities. Such security concerns present risks not only to the effective management of immigration, but provides new opportunities for human traffickers and the movement of terrorist cells.

Threat to threat

The scale of cyber fraud and online identity theft is significantly challenging the capability of police forces. According to the recent Crime Survey of England of Wales, cyber fraud continues to be the most prevalent crime in the UK, with people ten times more likely to become a victim than they are to suffer a traditional theft.

The scale of cyber fraud is rising, moreover, identity theft hit a record high of 174,523 incidents last year – and the vast majority of it happened online. According to the latest report by the Credit Industry Fraud Avoidance System (Cifas), the leading national non-profit fraud prevention service, identity theft has risen 125 per cent since 2007, representing a decade of unprecedented growth.

Separate research conducted by the virtual private network comparison site Top10VPN.com found that fraudsters operating on the Dark Web could buy a person's entire identity for just £820. Bank account details and Airbnb profiles are also of value to criminals who operate in the shadows of cyber space, while online bank details are currently worth around £168 to Dark Web bidders. Paypal logins fetch a higher price of about £280, with passport details attracting as little as £40. Hacked web accounts – such as access to your Match.com profile, Facebook and even Deliveroo – give cyber criminals a backdoor into identity theft for less than a fiver.

Mobile malware

According to Europol, the rapid development of mobile communications provides a larger attack surface for cyber criminals to target their efforts. Organised Cyber Crime Groups (OCCG's) are increasing their volume of mobile malware and rogue mobile applications as half of the world's adult population now own a smartphone. The technological advancements of the smartphone have made it the go-to device over the computer, and the one to which people are always connected.

For the policing of post-Brexit borders in the UK, the challenge becomes amplified as airline and sea transport companies have adopted mobile software for booking flights and ferries, offering online check-in facilities which requires the sharing of personal passport and banking information. Cybercriminals are increasingly looking to exploit this change in user device preference by switching an expanding proportion of their attacks to mobiles. As a result, more standalone attacks on mobile devices are expected in the future which presents a real and present menace to the individual smartphone user and to the safety and security of our borders.

Research to reality

As organised online identity thefts continue to grow more targeted and more advanced, police officers, academics and private industry partners are working together to counter these threats through ARIES (reliAble euRopean Identity EcoSystem), a research and innovation project funded by the Horizon 2020 Secure Societies programme of the European Commission. ARIES seeks to achieve a reduction in levels of identity fraud, identity theft and other related cybercrimes by creating a new system to improve the security of personal online data.

The ARIES consortium is made up of nine European partners from government, academia and private industry representing six EU Member States, and includes operational practitioner perspectives provided by police forces in Belgium, Spain and the UK. Together, they are developing a new system which strengthens the link between physical documents, biometric identity and the digital and mobile identity to prevent impersonation to reduce types of identity fraud and identity-related crimes. In addition they also aim to help victims of such crimes by assisting in the recovery of their virtual identities by the development of a "secure vault" for storing virtual identities whilst underpinning all of these innovations is the desire that this increase in security is a "trade off " against citizens' rights by ensuring at the same time security is increased civil rights are protected.

The validity of the ARIES approach is currently being tested and evaluated by two scenarios that will allow an opportunity for the ARIES consortium to prove a reduction in associated crimes. One test scenario centres on e-commerce whilst the other focuses on ID fraud issues within an airport context. The strategic objectives of the project directly respond to the need to increase the protection of personal data, and in particular individual identities, which remain highly vulnerable in the virtual world.

Working together

The uncomfortable truth from current cyber threat and risk assessments indicate that criminals are moving faster than the practical and operational implementation of effective cyber defences and counter measures. This position is unlikely to change and any new systems that can be used to strengthen existing security measures, while reducing the number of offences, victims and demand on precious police resources, must be welcomed.

The policing of our borders post-Brexit will pose immediate day-to-day challenges for policing. Security policy-makers and Brexit negotiators are acutely aware that both the UK and the EU risk becoming weaker and less secure if Brexit negotiations provoke a 'zero-sum' approach to security. That said, the collaborative ethos of project ARIES, with police, academia and private industry across Europe working together, provides a positive way forward, and presents a real opportunity to combat the threats to our borders from online identity theft, providing practical solutions that work for the effective post-Brexit policing of our ports and borders.

Dave Fortune

Director, Saher (UK) & ARIES consortium partner

ARIES (Reliable European Identity Ecosystem) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700085