CSI 30: Should we worry about cybercrime?

Summary

- In a world based on information technology, concerns about cyber-risks are highly prevalent
- The majority of Europeans perceive that the risk of cybercrime victimisation is increasing, demonstrating a widespread lack of confidence in data security
- In 2016, a larger proportion of fraud incidents in England and Wales involved cybercrimes than offline crimes

What types of cybercrime exist?

Computer-based crimes include many forms of illegitimate behaviour, including payment card fraud, general computer-based fraud such as fake shopfronts, and online hate speech. Different types of cybercrime target divergent victims: firms and state institutions are the predominant targets for data exfiltration (the acquisition of access to confidential information), while both individuals and organisations can be victimised by online extortion, spam, and malware (viruses). As Figure 1 illustrates, most Europeans use the Internet regularly, and over half use the internet for online banking and e-commerce, both critical tasks targeted by cyber criminals. With contemporary life hinging on the Internet and digital communications, it is unsurprising that "cyber" has become a new avenue for criminals.

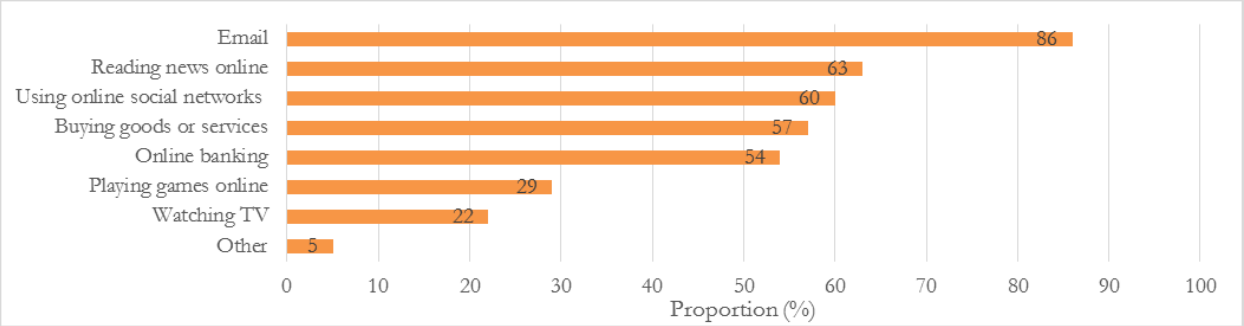

Figure 1: Online activities are highly prevalent in the EU, *Source: Eurobarometer, 2014*[1]

Most computer crimes are old crimes adapted to the current world. While the general principles behind many crimes are unchanged, criminals now use computers and the internet to work more efficiently and across territories. The level of anonymity on the Internet and the large number of unsuspecting victims simplify these activities. Fraud is the most common computer crime, and functions similarly in the cyber and physical worlds. Bank card fraud involves copying means of payment at modified point of sale devices in shops, skimming cards in modified cash machines, or by creating fake payment providers. These methods are the online equivalent of cheque forgery. The second main avenue for fraudsters is to mimic a trusted organisation such as a bank, commonly by sending fake emails, either general spam or targeted attempts (called *phishing*), to then extract payment from unsuspecting victims.

There also exist truly new crimes that are based on information technologies, usually classed as *computer misuse* in the UK. Such crimes include illegally breaching computer systems to acquire information, or the deployment of malware meant to destroy data or disturb operations. In 2015, so-called ransomware became a new avenue for cyber-criminals; this type of malware infects computers and encrypts (scrambles) data. Criminals then extort the victims who pay to receive a decryption key needed to retrieve their data. In May 2017, NHS computers were among the 500,000 worldwide infected by the ransomware *WannaCry*, which caused widespread delays in treating patients. Like most malware, *WannaCry* exploited bugs (errors) in software to spread and infect computers, a mechanism similar to the spreading of biological viruses.

Cybercrimes may also be aimed at designated targets. Advanced Persistent Threats (APTs), for example, are qualitatively different from opportunistic computer crime, and involve a team of specialists who target an organisation to find and exploit specific weaknesses, for example to steal classified information. APTs are costly, with substantial basic setup costs. The United States government recently accused the Russian government of interfering with the 2016 US presidential election using APTs, and expelled Russian diplomats amid these allegations. Another common threat is a Distributed Denial of Service attack, where requests that require bandwidth and computing time to process are continuously sent, causing overload. Servers consequently become unable to respond to legitimate requests, forcing organisations to rescind access to websites or services during the attack and thereby reducing profits.

Illegal material such as child pornography, drugs, and malware, is increasingly traded over the internet. Online marketplaces and forums have higher levels of anonymity than physical interactions, although this anonymity presents challenges in building trust and trading successfully. Buying fake merchandise, or being scammed is likely. Forums trading in illegal material are increasingly located on the so-called Darknet. Special software like The Onion Router (which conceals the user's location, making their activity difficult to trace) is needed to access the Darknet, which in combination with its strong encryption and anonymisation techniques, means that the Darknet offers protection and anonymity from law enforcement and the criminal competition. The use of Darknet sites has grown as the required tools are increasingly available, secure, and user-friendly. However, not everything on the Darknet is criminal: it is widely used by investigative journalists and at-risk populations such as activists in authoritarian states who need to protect their privacy.

How many people are affected by cybercrime?

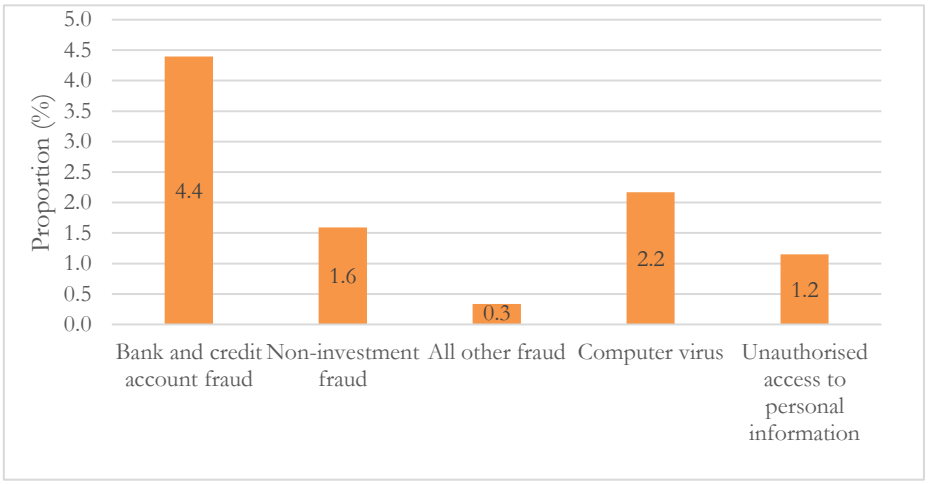

Figure 2: Bank and credit account fraud is more prevalent than computer viruses in England and Wales. *Source: Crime Survey for England and Wales, 2016*[2]

According to the National Crime Agency, there were 2.46 million cyber incidents and 2.11 million victims of cybercrime in the UK in 2015[3]. The Crime Survey for England and Wales included cybercrimes for the first time in 2016, revealing that 55 per cent of fraud incidents involved cybercrime[4]. Figure 2 shows that nearly one in twenty people in England and Wales reported being the victim of bank and credit account fraud, while other forms of cybercrime are less prevalent. Rates of cybercrime vary widely between countries. In the US, 64 per cent of survey respondents in 2016 reported falling victim to cybercrime, 41 per cent reported credit card fraud, and 35 per cent had experienced data breaches of personal information such as financial data or social security numbers[5]. The considerable discrepancy between reported cybercrime prevalence in the US and England and Wales is noteworthy, and will reflect both differences in the prevalence of cybercrime alongside the broader crime categories used in the US survey. Payment card fraud is doubtlessly more common in the United States due to the use of low-security magnetic stripe technology. US Social Security Numbers (which have no equivalent in the UK) also present an easy target, as these numbers are widely used and never change.

What are the consequences of cybercrime?

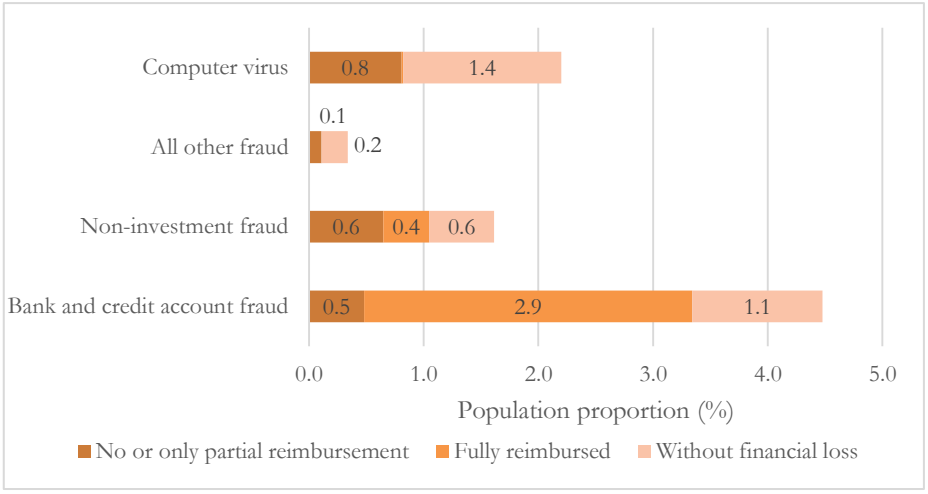

Figure 3: Reimbursement for financial damages is most prevalent for bank and credit account fraud, *Source: Crime Survey for England and Wales, 2016*[4]

For those affected, what happens after becoming a victim of cybercrime is important. Figure 3 shows that bank and credit account fraud is the most prevalent computer crime in England and Wales, with 4.4 per cent of the population reported being victimised in 2016. Reimbursement of damages is common for such crimes, where over half of victims are fully reimbursed for their losses. This high prevalence of reimbursement reflects the long-standing history of bank and credit account fraud – which existed long before cyber methods were developed – meaning that compensation measures have been necessary for decades. In contrast, insurance schemes against other cybercrimes are in their infancy, and reimbursement consequently less common: only one-quarter of non-investment fraud victims were fully reimbursed, while over one-third of computer virus victims received no or partial reimbursement. On the other hand, significant proportions of cybercrimes (including online bullying and accessing sensitive data) are defined as *without financial loss*, meaning they impose no direct financial damages. However, such crimes often lead to confidential information being compromised, which can increase vulnerability to identity theft or fraud at a later time, and may have wider impacts, such as psychological distress.

What is the impact of cybercrime on business?

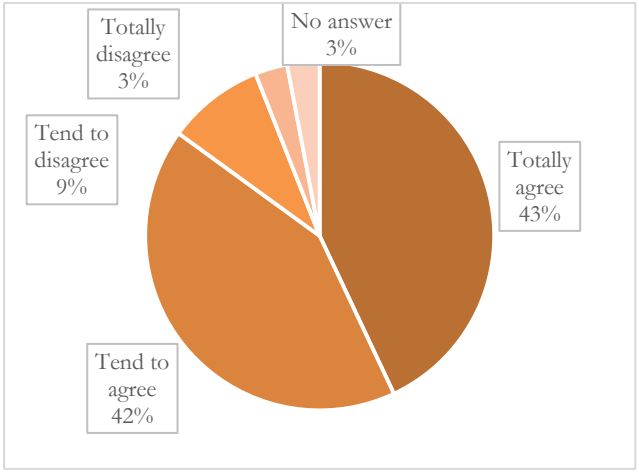

Figure 4: Europeans show high levels of agreement with the statement "*you believe that the risk of becoming a victim of cybercrime is increasing*", *Source: Eurobarometer, 2014*[1]

As Figure 4 underlines, the majority of Europeans believe that cyber-risks will increase. Similarly, over two-thirds of US survey respondents reported that they expect attacks on public infrastructure and banks[4]. Further evidence that 73 per cent of Europeans are concerned with website security and 67 per cent with the safety of information held by public authorities demonstrates considerable lack of confidence in online and data security. Such concerns may impact on people's use of online services and thus affect business. In addition to the losses from successful attacks, and the insurance schemes needed to cover damages of fraudulent activity, some businesses invest considerable resources in securing and protecting their networks, while others are dangerously careless. In future, retaining the trust of consumers and businesses in IT infrastructures will be vital for companies and state organisations but also the economy more generally.

Measurement Problems

Accurate measurement is a considerable problem in computer crime, as both quantitative and qualitative data are usually limited in scope and incomplete. Because some victims are unaware of having been victimised, representative surveys of victims are near impossible. Many companies also prefer not to report breaches or attacks for public image reasons. Results from a 2016 survey revealed that 39 per cent of UK respondents who said they had experienced cybercrime had not reported the incident[5]. Cybercrimes were included in the Crime Survey for England and Wales for the first time in 2016, but these figures are currently considered experimental and do not have the status of National Statistics. Meta-data like computer addresses and connection records, are sometimes useful for law enforcement and security researchers. This reflects the attribution problem: even if the computer used to compromise a system can be identified, this does not mean that the computer's owner is necessarily behind the attack. It could instead have been used remotely and without permission by someone else.

What measures are used to address cybercrime?

Amid huge potential losses, many organisations have invested heavily in recent years: common security measures include specialised teams that continuously monitor networks, improved system architectures, more sophisticated automated systems, and security tests and audits. Increased cooperation among companies and state actors has also improved the situation. For example, the UK financial sector shares information and intelligence among competitors. The empowerment of police forces is another important step towards stronger enforcement; examples include Europol with their cybercrime centre EC3, which coordinates law enforcement against IT crimes across borders, and the National Crime Agency, the UK agency specialising in cybercrime. The fight against online crime shows promise but policing the internet remains work-intensive due to online anonymity, the lack of international cooperation, and sufficient investments in some countries. A combination of more effective law enforcement and increased defensive efforts is needed to discourage online criminality.

Why is cybercrime here to stay?

IT security provision is complex and multi-dimensional, making defence efforts expensive and labour intensive. In contrast, cybercriminals face fewer challenges than traditional offenders: they can operate across borders while being physically based in countries with poor protection against cybercrime. They can also take advantage of technical measures that hide their identity and location (such as The Onion Router), significantly reducing the probability of detection. While considerable progress has been made recently, whether companies and different national police forces will cooperate gainfully and adapt quickly enough to new challenges in cybercrime remains to be seen. Human error and credulity are common reasons for successful attacks and malware infestations, yet product design and lax security provisions are also to blame for successful attacks and continued losses. Companies face little to no repercussions either for data breaches or releasing products with insufficient security measures. Stricter regulation and security requirements could increase the pressure on companies to inhibit criminal activity. Targeted and advanced attacks are more difficult to discourage, but stronger IT security regulation and enforcement would make such attacks trickier to execute, pricing some actors out of the market.

Author: Laurin B Weissinger
Acknowledgements: With many thanks to Elisabeth Garratt for her helpful comments.
Publication date: July 2017

[1] *Eurobarometer 82*, 2014 Available at: http://ec.europa.eu/COMMFrontOffice/downloadODP/?4ADEAE2F2C0C62FF78D6EF3D7EB1C34C
[2] Office for National Statistics (2016) *Crime Survey for England and Wales, Experimental Statistics Table E1.*
[3] NCA Strategic Cyber Industry Group (2016*) Cyber Crime Assessment 2016*, Available at: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
[4] Office for National Statistics (2016) *Crime Survey for England and Wales, Experimental Statistics Table E2.*
[5] K. Olmstead and A. Smith (2017) *Americans and Cybersecurity.* Available at: http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf
[6] Get Safe Online (2016) https://www.getsafeonline.org/news/fraud-cybercrime-cost-uk-nearly-11bn-in-past-year/