Financial Crime & Cyber Security: The Power of Data

Professor Gerhard Kling

University of Aberdeen

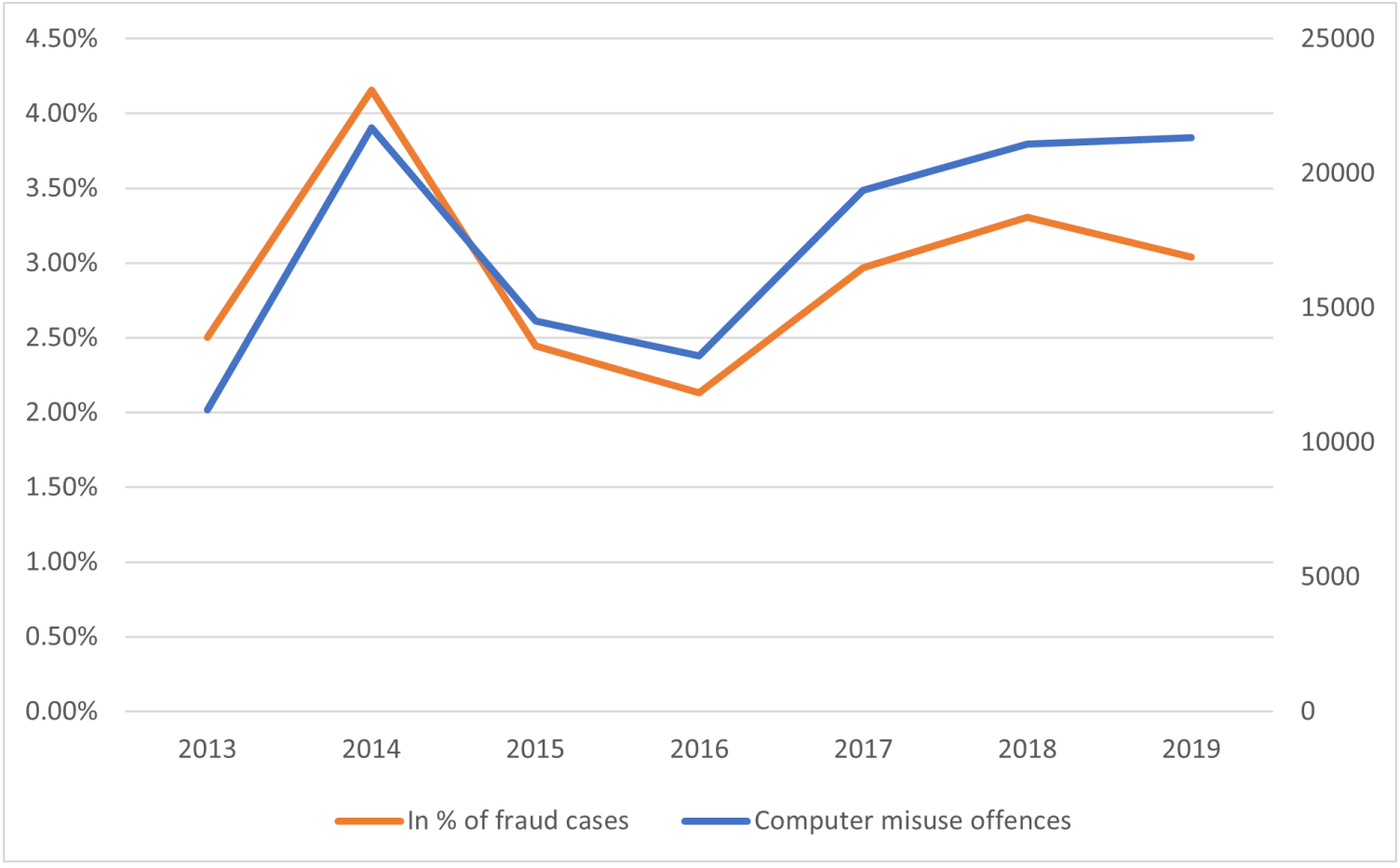
June 12, 2022

What is cybercrime?

- Defined in the Counting Rules published by the Home Office
- Virus, malware & spyware
- Denial-of-service attacks
- Hacking of personal computer
- Hacking of social media & email
- Hacking of PBX/dial through
- Hacking combined with extortion
- DDoS or denial-of-service attacks occur if an attacker disables a service (e.g., Google Cloud 2017, Amazon Web Services 2020)
- PBX (Private Branch Exchanges) are less well known forms of attacks, where hackers target telephone systems of companies to make expensive calls

The scale of the problem

- The 'Nature of fraud and computer misuse in England and Wales' is the only dataset available from the Office for National Statistics (ONS)
- Action Fraud reports 31,322 cases in 2020/21 with $\frac{1}{3}$ social media and email hacking. Losses were £9.6 million



Research on cybercrime

- As outlined by [1], more than a third of Internet users in the UK reported a 'negative online incident' in 2011/12 - but most cases including virus attacks were not recorded as crimes
- More recent empirical research has focused on the COVID-19 pandemic and the alleged increase in online crime. [3] argue that changes in individual behavior such as an increase in online retail have contributed to a higher exposure to cybercrime. [2] provide a recent international overview of cybercrime.

Checking for leaks: Emails, mobile phones & passwords

- https://haveibeenpwned.com; Check your emails and mobile phones
- https://haveibeenpwned.com/Passwords; Check your passwords
- https://www.avast.com/hackcheck/; Check your emails; covers website hacks
- Password managers https://www.lastpass.com

Your IP address

- SOHO (small office / home office) network
- Sources of vulnerabilities: (1) Internet, (2) Devices on your network (e.g. mobile phones), (3) Wireless
- Public IP address - check it on https://whatismyipaddress.com/ - you can be easily identified
- Test for vulnerabilities: https://pentest-tools.com/home then click on scan your network; it uses your public IP address; main risk if you run a website using one of your devices a port is open; this is based on `NMap`, which is open source

Identity theft in the UK

- Lack of system for registration
- Demonstrate proof of address using utility bills etc.
- Lack of photo IDs
- Limited checks lead to fraud
- Check credit reports regularly https://www.clearscore.com/ - this service is free
- Checks include dark web searches

Are you a money mule?

- Young people are targeted
- Offers of work experience
- Remote working
- Handling mail & deliveries
- Buying & selling electronic products (e.g., apps)

Can you be identified online?

- Test your browser security: https://coveryourtracks.eff.org/
- How many bits of information denoted ΔS is needed to identify a person among 7.8 billion users? The answer is given in Information theory (Shannon entropy and is about 30 bits, i.e. $\Delta S = -\ln \Pr(X = x)$
- Also some of the information we leak is incorrect when using VPNs and TOR

What does a VPN do?

- Many providers, e.g., https://www.privateinternetaccess.com/
- Data send from your computer to the VPN computer encrypted
- But traffic from the VPN to other sites is not encrypted!
- Thus you can create a secure tunnel using first a VPN and then connect to the Tor network
- Do not rely on free providers and make sure you use HTTPS (Hypertext Transfer Protocol Secure) (TLS encryption) in every connection
- Check how much information your VPN provider has, e.g. name, address etc.
- Alternative more private providers (e.g., payment with cryptos)

Is a VPN sufficient for your security?

- Main issue is that metadata is sufficient evidence
- Example: your internet service provider (ISP) knows when you access www.youtube.com - but they do not know which video you watch
- VPN providers store data based on your transaction (e.g., credit card)
- VPN providers have similar access compared to ISPs

Do we need more regulation?

- Online Safety Bill
- "Platforms likely to be accessed by children will also have a duty to protect young people using their services from legal but harmful material"
- Risks might lead to less information online
- More rules - more enforcement of rules - or more education?

The power of data

- Data is everywhere - can be used to detect fraud and unsafe connections etc.
- Learn to use data effectively (e.g., Data Science)
- Learn programming!
- Python is the way!


Julio Hernandez-Castro and Eerke Boiten, *Cybercrime prevalence and impact in the uk*, Computer Fraud & Security **2014** (2014), no. 2, 5–8.


Thomas J Holt and Adam M Bossler, *The palgrave handbook of international cybercrime and cyberdeviance*, Springer, 2020.


Steven Kemp, David Buil-Gil, Asier Moneva, Fernando Miró-Llinares, and Nacho Díaz-Castaño, *Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during covid-19*, Journal of Contemporary Criminal Justice (2021), 10439862211027986.