Scottish Government
Riaghaltas na h-Alba
gov.scot

Cyber-crime in Scotland: A Review of the Evidence

CRIME AND JUSTICE

social
research

Contents

Cyber influence on crime: Summary of overall findings

Cyber-technology can impact on any type of crime. We conceptualise cyber-crime in terms of the method or locus of a crime, rather than it being a distinct type or group of crime.

From the available evidence, we know that:
Cyber-technology has had an **impact** on

The scale and nature of some types of **sexual crimes** in Scotland

The proportion of **fraud** conducted online. However still a lot of fraud is offline. As a whole, fraud is under-reported and mostly low impact

Computer misuse – now a commonly experienced crime. But it is under-reported and mostly low impact.

There has been **less influence** of cyber-technology on the following:

Cyber appears to have no real influence on the scale and nature of **violent crime**

Drugs are still mainly sourced via traditional means rather than online.

The internet features in cases of **stalking and harassment** but this is still more prevalent in-person than online.

Information of **businesses'** experiences of cyber-crime is limited and fragmented, however most sources indicate that cyber-crime is an issue for them.

For example, the UK Cyber Breaches Survey, whilst not covering all sectors, estimates that between 2016 and 2017, **46%** of responding business sectors experienced at least one cyber breach or attack.
(Cyber Breaches Survey, 2017.)

Justice Analytical Services

Executive Summary

Purpose

This desk-based review aims to contribute to the evidence base and aid understanding of how cyber-technology is impacting on crime in Scotland.

The review is set against the backdrop of a number of recently published strategies which emphasise the challenges and risks of cyber-crime. These include the Scottish Government's Justice Vision and Priorities, Cyber Resilience Strategy and Policing 2026.

To inform this on-going strategic work, a number of analytical workstreams are being undertaken across a range of organisations and this evidence review marks the Scottish Government's contribution to the initial phase of developing an evidence base.

Structured according to recorded crime groups, the review summarises key evidence from a number of existing Scottish and UK sources. It focuses on how cyber-crime is measured, the nature and extent of cyber-crime, apparent evidence gaps and potential evidence sources going forward. The review firstly considers crimes impacting individuals before turning attention to businesses.

What is cyber-crime?

Defining cyber-crime is complex and contentious and there is not an agreed upon definition[1].The main debate centres around the extent to which the internet and cyber technologies need to be involved in order for the crime to be termed 'cyber-crime'. Views on this range from those who argue that cyber-crime is only the distinct set of activities which are committed by using a computer, computer networks or other forms of ICT (e.g. spread of viruses, hacking etc.), to others who view cyber-crime as including even the most minor involvement in more traditional crime types (e.g. using the internet to research how to commit or cover up a violent crime).

Given the remit of this review and the broader cyber-crime analytical work, it makes most sense to adopt a definition that considers criminal activity as cyber-crime if cyber-technology was in any way involved, regardless of the extent of involvement. This approach does not necessarily consider cyber-crime as a separate category of crime, instead it is defined by the method or locus of the crime. This is in line with the way in which Police Scotland conceptualise cyber-crime.

[1] Wall, D.S., (2017). Crime, Security, and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and its Implications for Regulation and Policing.

Context - Internet use in Scotland

In order to set the subsequent findings in context, it is important to consider the broader picture in terms of levels of and trends in internet use across Scotland. Whilst the growth of the internet has created many positive opportunities, these are accompanied by inherent risks and the potential to be exploited by criminals.

- The vast majority of adults in Scotland (84%) reported using the internet for personal or work use in 2016, this figure has remained stable of late but has significantly increased since the 2007 baseline year of 63%[2].
- There is a clear relationship between internet use and age, with use increasing as age decreases. Usage also tends to increase in line with household income.
- There are indications that the public are aware of the potential risks of using the internet, with the majority taking precautions to protect themselves. In 2016 only 7% of internet users noted that they adopt no security measures[3].
- The 2017 Cyber Security Breaches Survey found that 74% of UK businesses[4] consider cyber security to be a high priority for senior management[5] and fewer firms now say it is a very low priority compared to 2016.
- The same survey revealed that the vast majority of UK businesses have cyber security measures in place including applying software updates (92%), malware protection (90%) and firewalls (89%).

Key findings- Crimes affecting individuals

The following provides an overview of the key findings to emerge from the review. Please see the glossary at the end of this paper for definitions of the terms used.

Non-sexual crimes of violence

- The available evidence suggests cyber technology appears to be having no significant influence on the scale or nature of non-sexual crimes of violence.
- There is insufficient evidence to assess the role of cyber technologies in cases of threats and extortion in Scotland.

Sexual crimes

- Cyber technology has had an impact on both the scale and nature of sexual crime in Scotland.
- Estimated that the internet was used as a means to commit at least 20% of all sexual crimes recorded by the police in Scotland in 2016/17.

[2] Scottish Household Survey, 2016

[3] Of those asked about in the Scottish Household Survey

[4] Representative of businesses in scope of the survey, excludes some sectors and businesses with no IT capacity.

[5] 31% very high, 43% fairly high

- Online sexual crimes tend to be concentrated around non-contact offending but the internet may be a precursor in contact sexual crimes e.g. rape, sexual assault.
- Both the number and proportion of police recorded ‘other sexual crimes’[6] which were cyber-enabled (internet used as a means to commit the crime) has increased. In 2016/17, 51% of ‘other sexual crimes’ were cyber-enabled, up from 38% in 2013/14[7].[8]
- This increase has contributed to the growth in police recorded ‘other sexual crimes’, and sexual crimes as whole between 2013/14 and 2016/17.
- When the specific ‘other sexual crimes’ of ‘communicating indecently’ and ‘cause to view sexual activity or images’ are cyber-enabled:
- Victims and offenders tend to be younger (compared to non-cyber cases), with the majority of victims aged under 16.
- Victims and offenders are more likely to know of one another.

Fraud

- Evidence suggests that fraud is one of the most numerous crime types, but this is <u>not entirely</u> driven by the internet.
- Evidence from the Scottish Crime and Justice Survey (SCJS) shows in 2014/15, 5% of adults reported that they were victims of bank and credit account fraud. This has increased in recent years but the data is subject to caveats.
- Crime Survey for England and Wales (CSEW) data shows 3.2 million incidents of fraud were experienced by 5.9% of adults in the year ending Sept. 2017.
- For the year ending Sept. 2017, the CSEW estimates 56% of fraud incidents were coded as cyber (internet or any type of online activity related to any aspect of the offence), amounting to an estimated 1.8 million incidents.
- As yet no victimisation survey has published data looking specifically at the victims, impacts and reporting of fraud committed via the internet. This could reflect methodological challenges.
- Incidents of fraud (on and offline) are underreported to Action Fraud and the police. This is possibly linked to incidents generally being viewed as having no emotional or physical impact or as an inconvenience (rather than anything more harmful), in addition to the relatively high rates of financial reimbursement.

[6] This is one of four categories Police Scotland use to record sexual crimes - the other three being ‘Rape and attempted rape’, ‘Sexual Assault’ and ‘Crimes associated with prostitution’. ‘Other sexual crimes’ are made up of a wide range of sexual crimes, with the three most common being ‘Communicating indecently’, ‘Cause to view sexual activity or images’ and ‘Indecent photos of children’.

[7] Based on a sample of crimes recorded by the police.

[8] Recorded Crime in Scotland: Other Sexual Crimes, 2013-14 and 2016-17.

- There is insufficient CSEW time series data in order to establish any trends in the incidence and nature of fraud including the role of cyber technology.

Computer misuse

- The term ‘computer misuse’ is used to capture a number of crimes generally covered by the Computer Misuse Act 1990. Activities grouped under this label mainly centre around unauthorised access to and (sometimes subsequent) attacks on computer systems, networks and data e.g. hacking, computer viruses and Distributed Denial of Service (DDOS) attacks.
- Whilst evidence shows computer misuse to be numerous and fundamentally driven by the growth of cyber technology and the internet, in most cases there is either no resulting impact or such impacts tend to be of low severity.
- The most robust and comprehensive evidence on computer misuse is data gathered via the CSEW, which incorporates incidents of unauthorised access to personal information (including hacking) and computer viruses.
- CSEW evidence shows 1.5 million incidents of computer misuse were experienced by 2.6% of adults in the year ending Sept. 2017.
- Almost all (97%) incidents were coded as cyber (internet or any type of online activity related to any aspect of the offence) for the year ending Sept. 2017, amounting to an estimated 1.46 million incidents.
- Victimisation of computer misuse is generally spread across society but some groups are more at risk including higher income households.
- CSEW evidence shows that in 49% of computer misuse incidents victims identified no resulting emotional or physical impacts and by far the most common impact was a ‘loss of time/inconvenience’, experienced in 31% of incidents (year ending March 2017)[9].
- Police recorded crime data for Scotland suggests that incidents of computer misuse are underreported. In 2016/17 only 30 incidents were recorded under the Computer Misuse Act 1990.

Other crimes

- Available evidence suggests the vast majority of illicit drug users are still sourcing drugs via traditional means, with a very small proportion obtaining drugs online.
- Concerns that increases in the amount and accessibility of information online would increase the likelihood of contempt of court issues (e.g. jurors finding out information about a case), have yet to be borne out in police data.

Miscellaneous Offences

- Evidence suggests that the internet may commonly feature in cases of stalking and harassment, yet being pestered, intimidated or insulted in-

[9] Emotional and physical impact on victims of incidents of computer misuse, Year ending March 2017, CSEW

person is much more prevalent than experiences carried out via electronic means.

- SCJS evidence indicates that of the 9% of adults ‘insulted, pestered or intimidated’ in Scotland in 2014/15, the vast majority (82%) experienced this in-person.
- SCJS evidence shows that in 2014/15, the most common type of stalking and harassment (arguably more serious than the above) was threatening/obscene texts or emails, experienced by 45% of adults who had encountered at least one form of stalking/harassment in the 12 months prior to interview (6.4%).
- Evidence suggests incidents of harassment and threatening/abusive behaviour are underreported to the police, with many viewing it as ‘too trivial’.

Key findings- crimes affecting businesses

- Many organisations collect data on the impact of cyber-crime on businesses, however as there is not consistency in how these data are collected across these organisations, it is not possible to present a robust overview of the impact of cyber-crime on business. Nevertheless, it is clear from the available evidence that cyber-crime is an issue for businesses.

Fraud

- In spite of the challenges highlighted above, it is clear from the available evidence that fraudulent acts are frequently experienced by businesses.
- The 2017 Cyber Breaches Survey found that staff receiving fraudulent emails or being redirected to fraudulent websites was the most common type of cyber breach experienced by UK businesses covered by the survey.
- The 2016 Retail Crime Survey revealed fraud to be the second most commonly experienced crime amongst respondents, accounting for 18% of incidents.
- Evidence suggests the costs of online fraudulent activities are smaller than costs associated with traditional crimes and amount to a minority of total online transactional values.
- The 2016 Retail Crime Survey estimated that 53% of the total cost of fraud was cyber-enabled, representing a total direct cost to the retail industry of around £100 million. This translates to approx. 15% of the total direct cost of crime against retailers.
- UK evidence from Financial Fraud Action shows in 2016, fraud losses as a proportion spent on UK issued cards stood at 8.3 pence per £100.
- For 2016 Financial Fraud Action estimated value of transactions carried out online using fraudulently obtained cards accounted for 9.5 pence in every £100 spent with UK merchants.

Computer misuse

- ‘Computer misuse’ is used to capture a number of crimes generally covered by the Computer Misuse Act 1990 and incorporates activities such as unauthorised access (e.g. hacking) and attacks (computer viruses).
- The UK-level 2017 Cyber Breaches Survey estimates that 46% of businesses identified at least one cyber breach or attack between 2016 and 2017, but this data is subject to caveats.
- Incidence of such breaches increases with businesses size (number of employees) and turnover, in addition to varying by sector.
- The attractiveness of personal customer data to criminals could be increasing the risks for companies holding such information. The 2017 Cyber Breaches Survey found that 51% of UK businesses holding personal customer data experienced a breach, compared to 37% who didn’t hold this information.
- Evidence from the UK 2017 Cyber Breaches Survey shows where businesses experience a breach, incidents of computer viruses, spyware and malware (33%) in addition to Ransomware (17%) are amongst the most common.
- Evidence suggests that staff are viewed as pivotal in the prevention of cyber attacks but are also potentially a weak link in businesses’ defences.
- Very few businesses have systems in place to calculate the costs of cyber attacks and there is a lack of consistency in previous research which attempts to estimate costs.
- The majority of businesses identifying a breach do not report them to external bodies and even less report them beyond their cyber security provider. The main reason is that incidents or the impact were thought to not be significant enough.

Conclusions

This review has drawn attention to the increase in the number of people in Scotland using the internet and the potential for criminals to exploit this growth, under the banner of cyber-crime. There is a lack of clarity and consistency in the terminology used around cyber-crime, and moving forward it may be helpful to start to shift the focus towards cyber-crime being seen as the method or locus of a crime, rather than a distinct type or group.

Whilst this review has found that incidents of cyber-crime tend be concentrated around sexual crimes, fraud and computer misuse, a number of different types of crime can and likely do involve the use of the internet and cyber technologies, either as a precursor to a crime or in the committing of a crime itself.

The review has highlighted four key ways in which cyber technology is influencing crime:

1. **Cyber-crime is forming a large proportion of certain crime types.** For example evidence from the CSEW for the year ending Sept. 2017 estimates that over half (56%) of fraud incidents (which is one of the most numerous crimes) were cyber-crimes. This amounts to 1.8 million incidents during this time period.

2. **The internet and cyber technologies are changing the volume of certain crime types.** This is perhaps most evident amongst sexual crimes. Detailed evidence shows that both the number and proportion of police recorded ‘other sexual crimes’ in Scotland which were cyber-enabled increased. Consequently such incidents contributed to the growth in all ‘other sexual crimes’ and sexual crimes as a whole.

3. **The internet and cyber technologies are changing the nature and victimisation of certain crimes.** The police recorded ‘other sexual crimes’ research found that when the specific crimes of ‘communicating indecently’ and ‘cause to view sexual activity or images’ were cyber-enabled, both victims and offenders tended to be younger compared to non-cyber incidents. With cyber-enabled incidents, victims and offenders were also more likely to know of one another.

4. **Cyber-technologies have given rise to the introduction of an entirely new and high volume category of crime – computer misuse.** Without the internet, these crimes (including computer viruses, hacking etc.) would not be possible. Evidence from the CSEW for the year ending Sept. 2017 shows there were 1.5 million incidents of computer misuse, making it one of the numerous crimes.

However, we are operating in a complex landscape. The review has drawn attention to the challenges faced by authorities to investigate and take action against online risks. These include inconsistent terminology and the spectrum of possible internet involvement in crimes. Such situations also challenge the capability of research and statistics to accurately capture the scale, nature and impact of cyber-crime.

This review has also identified gaps in our knowledge. We still need to know more about cyber-crime in Scotland, such as the prevalence of different types of cyber-crime, the extent of underreporting, the cost and the harm of cyber-crime. Furthermore little evidence is available which allows for the comparison between cyber and non-cyber incidents of the same crime. This review has also drawn attention to gaps around cyber-crime offenders, in particular the extent to which different kinds of individuals and groups account for cyber-crime offences in Scotland.

Throughout, this review has found evidence that cyber-crime is underreported to the police and other authorities. Figures from the victimisation surveys are consistently higher than in police data, most notably for instances of fraud, computer misuse, abusive/threatening behaviour and stalking and harassment. Suggesting these occurrences are often not being reported to the police. Where apparent, the review has highlighted the possible links between underreporting and the perceived low severity of impacts resulting from many incidents, especially in relation to fraud and computer misuse. Underreporting may be inhibiting the ability of the police to take action and to assign resources accordingly.

Next steps

In addition to this review, a number of analytical workstreams are being taken forward across numerous organisations, including:

- Police Scotland Cyber Capability Review;
- Scottish Institute of Policing Research (SIPR) qualitative research which looks at policing practices from six different countries around the world; and
- HMICS Thematic Inspection of Police Scotland response to Cyber-crime.

Furthermore, there are some encouraging signs by way of emerging evidence sources in Scotland. Principal developments include:

- Police Scotland introduced a cyber-marker to their crime recording systems in April 2016. Police Scotland are currently considering how to enhance how crimes with a cyber-element are marked. Identifying a solution requires challenging the definitions and perceptions of “cyber-crime” and acknowledging the limitation of current legacy systems. Therefore improvement will be incremental as definitions and systems develop.
- The SCJS has the potential to capture crimes that are not reported to or recorded by the police. Whilst the SCJS does currently include a limited number of questions which provide insight on the extent to which the internet and cyber technology was involved in certain incidents, a more comprehensive module on cyber-crime/online behaviour questions will be included in the SCJS questionnaire from 2018/19. This represents an important step in developing SCJS evidence is this area[10]. More information is available in the SCJS 2018/19 Questionnaire Review Paper and the full 2018/19 questionnaire will be published in due course.
- It is likely that private companies and businesses including banks, hold useful information on cyber security and incidents where they have been the victim of a crime which occurred online or via cyber technology. The Scottish Government’s Justice Analytical Services division is looking to explore this further.

Going forward it is intended that these developments combined with the above analytical work and existing sources, will contribute to a more complete picture about the influences cyber-technology is having on crime in Scotland.

[10] Will provide indicative findings. Data will not be included in the main SCJS incident or prevalence estimates.

1. Introduction

Background

This review looks at existing evidence to understand how cyber-technology has impacted on crime in Scotland. A number of recent strategies have highlighted the challenges presented by cyber-crime and focus on improving the way in which we prevent and respond to cyber threats:

- Justice Vision and Priorities identified the challenges facing the justice sector over the next ten years. One of these challenges was emerging crime and threats such as cyber-crime.
- Policing 2026 sets out the current strategic policing priorities and objectives. One of the main priorities is to scale and change Police Scotland's cyber capability to respond to emerging cyber related crimes.
- The Scottish Government's Serious Organised Crime Strategy (2015) recognises that the nature of serious organised crime has changed due to the substantial increases in cyber-crime. Two of the Strategy's themes, relating to diverting and deterring people from being involved in serious and organised crime, aim to ensure that individuals are aware of cyber threats and are able to safely use the internet and social media, and that businesses are able to protect themselves from cyber threats, insider threats and fraud.
- "Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland (2015)" sets out a vision for Scotland to become a world leading nation in cyber resilience by 2020.

To support this strong focus on preventing and tackling cyber-crime, we need a sound evidence base underpinning our actions in this area. There is currently a range of analytical work being carried out across different organisations.

The full range of work currently on-going comprises:

- This **Scottish Government review of cyber-crime** and its impacts on Scotland, exploring existing evidence and literature (including the Scottish Crime and Justice Survey and official crime statistics).
- **Police Scotland Cyber Capability Review** to ensure Police Scotland has a strategic understanding of the cyber-crime threat, and ensure that policing at all levels is equipped to investigate and respond to cyber-crime and exploit digital and technological developments. This is a long term piece of work.
- **Scottish Institute of Policing Research (SIPR)** qualitative research which looks at policing practices from six different countries around the world. This is due to be completed in Spring 2018.
- **HMICS Thematic Inspection of Police Scotland response to Cyber-crime** – scheduled to be carried out in 2018-19.

This cross organisational analytical work is reflective of the scale and complexity of the challenge of cyber-crime. It needs a collective effort across organisations and sectors in order to develop a shared understanding. Taken together this work will begin to build a better understanding of the nature and scale of cyber-crime and how the risks, challenges and impacts of cyber-crime may differ from those associated with “traditional” crime (including whether there is now more crime in Scotland and/or whether the nature of crime committed has changed with the rise of the internet).

Aims of this evidence review

The Scottish Government’s contribution to this initial building of the evidence is to understand what impact cyber-technology has had on crime in Scotland. It looks at how cyber-crime is currently measured, what information we have and where measurement gaps are evident. This review does this by synthesising and condensing existing evidence around:

- The nature and extent of cyber-crime;
- Who are the victims of different types of cyber-crime;
- What harm is experienced by victims of different types of cyber-crime and the impact this has;
- Future plans for collecting evidence on different types of cyber-crime; and
- What we know about cyber-crime offenders.

This will then allow us to start developing options to improve the measurement and reporting of cyber-crime.

Structure of this evidence review

This evidence review is split into two main sections:

1. Cyber-crime as it impacts on individuals; and
2. Cyber-crime as it impacts on businesses.

This structure reflects the different kinds of risks and potential impacts faced by these two categories of victims. Within each, the review provides some background and contextual information before moving to consider the available evidence on the nature and extent of cyber-crime. For ease, this is organised by recording crime groupings. Whilst six crime groupings are discussed in relation to individuals, for businesses the review focuses on two. This is partly due to the available evidence and the fact that some crime groups aren’t applicable to businesses e.g. sexual crimes.

Recorded crime groupings

To understand how cyber-technology has impacted on crime in Scotland, this paper uses the crime groupings that are used to categorise police recorded crime statistics. This approach helps to contextualise evidence on the extent of cyber-crime within broader trends in categories of recorded crime, and also aids understanding of how cyber-crime is influencing crime, i.e. whether cyber-crime is replacing or adding to ‘traditional crime’. The table below sets out the crime groups along with a brief summary of the crime types that we consider could involve a cyber-element, and whether they affect individuals or businesses.

Types of cyber-crime by recorded crime groupings

Crime Group	Crime types affecting individuals	Crime types affecting businesses
1 – Non-sexual crimes of violence	• Serious assault • Threats & Extortion (although most cyber-related threats are expected to be in Group 6)	
2 – Sexual crimes	• Sexual offending – including child sexual exploitation and indecent communications	
3 – Crimes of dishonesty	• Fraud • Identity theft	• Fraud
4 – Fire-raising, vandalism etc.	• Computer misuse	• Computer misuse
5 – Other crimes	• Drug offences (e.g. trading of illicit substances online) • Contempt of court	• Intellectual property theft / copyright offences
6 – Miscellaneous offences	• Threatening communications & threatening and abusive behaviour • Stalking • Harassment • Bullying[11]	

As can be seen, the risks faced by individual victims in particular appear to be dispersed across the range of crime groups highlighting that cyber-crime captures

[11] Whilst not a specific crime type on its own, bullying relating to online experiences will be considered within Group 6 for the purposes of this paper given its shared characteristics with harassment and threatening and abusive behaviour. Whilst bullying can involve physical violence, the aspects which are suspected to be most commonly related to online experiences are considered to more directly relate to the existing crime types in group 6.

an array of various offences and experiences, which may have differing kinds of impacts and affect different groups of victims.

What is cyber-crime?

Defining cyber-crime is complex and contentious and there is not an agreed upon definition[12]. To fully understand the impact of cyber technology on crime in Scotland, it is important for us to set out what we mean by cyber-crime and the activities that fall under this umbrella term.

The main debate around whether criminal activity can be defined as cyber-crime centres around the extent to which cyber technology needs to be involved. Some argue that cyber-crime is only the distinct set of activities which are committed by using a computer, computer networks or other forms of ICT (e.g. spread of viruses, hacking etc.). Others consider cyber-crime as more of a continuum, with even the most minor involvement of the internet in more traditional crime types being considered cyber-crime (e.g. using the internet to research how to commit or cover up a violent crime).

As we are looking for this review and further analytical work to consider the impact that cyber-technology has had on crime in Scotland, it makes most sense to adopt a definition that considers criminal activity as cyber-crime if cyber-technology was in any way involved, regardless of the extent of involvement. In effect then, almost any crime has the potential to be cyber-crime. Therefore, this definition does not necessarily consider cyber-crime as a separate category of crime. Instead, cyber-crime is defined by the method or locus of the crime.

This is in line with the way in which Police Scotland conceptualise cyber-crime; they work with a continuum. This starts with traditional crimes conducted with a cyber-element and continues through to cyber-enabled crimes, i.e. those crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT, and then moves into completely cyber-dependent crimes. The Home Office also draw this distinction between cyber-enabled and cyber-dependent crimes but do not include crimes which have a lesser involvement of cyber technology.

[12] Wall, D.S., (2017). Crime, Security, and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and its Implications for Regulation and Policing.

2. Cyber-crime as it impacts on individuals

This review now turns to consider the evidence relating to cyber-crime as it impacts on individuals. Following some contextual information, the evidence is presented and discussed in relation to the six recorded crime groupings.

Main sources of evidence

Before considering the evidence on the nature and scale of cyber-crime in Scotland, it is important to briefly note the main evidence sources employed in this review, including technical details and known limitations. Such details should be borne in mind when considering the evidence from these sources.

Source	Details	Limitations
Scottish Crime and Justice Survey (SCJS)	• Large scale, representative social survey asked of 6,000 adults in Scotland each year. • Respondents asked about their experiences and perceptions of crime. • Includes a main questionnaire asked in a face-to-face interview and self-completion modules. • Crucially, it also includes crimes that have not been reported to the police. • Provides weighted estimates, including prevalence rates (the risks of being a victim). • Good measure of long-term trends.	• Does not cover the entire range of crimes and offences that the police are faced with. • Does not cover the entire population- is limited to crimes committed against adults (aged 16+) who live in private households. • Excludes those living in some of the smallest inhabited islands in Scotland. • Data from a sample of the population so subject to sampling error. • Survey dependent on respondents recalling past events.
Crime Survey for England and Wales (CSEW) – previously the British Crime Survey	• Large scale, representative social survey involving a sample of 50,000 households across England and Wales. • Includes a main questionnaire asked in a face-to-face interview and self-completion modules. • Since 2015, included module on fraud and computer misuse. • First year-on-year fraud and computer misuse data published in January 2018. • Includes 'cyber flag' questions in victimisation module. • Includes crimes that have not been reported to the police. • From 2009 the survey has included a separate	• Does not cover the entire range of crimes and offences that the police are faced with. • As with the SCJS it does not cover the entire population. • Findings will not necessarily be directly applicable to Scotland. • Data from a sample of the population so subject to sampling error. • Survey dependent on respondents recalling past events.

	survey asked of people aged 10-15. - Provides weighted estimates, including prevalence rates (the risk of being a victim). - Good measure of long-term trends.	- Further time series data is needed to establish any trends in fraud and computer misuse findings.
Police Recorded Crime in Scotland	- Statistics on crimes that are recorded by the police derived from administrative police records. - Collected by financial year. Statistics released in an annual publication. - Statistics grouped into seven groups (five crime groups and two offence groups). - Covers the full range of crimes and offences.	- Only includes crimes which come to the attention of the police, and this can be affected by reporting behaviours, public awareness, police activity and legislative changes. - More serious incidents/higher impact incidents might be overrepresented. - From April 2016 there has been a requirement to identify and record instances of cyber-crime using a defined marker. However this is still being implemented and developed. - Where it can be confirmed that the locus of an online offence is out-with Scotland then such occurrences, if already recorded will be classified as 'no crimes' (i.e. cases they were originally thought to be a crime but were later re-designated).
Police Recorded Crime in Scotland, 'Other sexual crimes' research	- Scottish Government research involving a random sample of around 2,000 'other sexual crime' police records from 2013-14 and 2016-17. - This represented 28% and 27% of all 'Other sexual crimes' recorded by the police in 2013-14 and 2016-17, respectively. - Sample was stratified by crime type to ensure the prevalence of the different types of sexual crimes recorded within the 'Other sexual crimes' category was reflected within the research.	- See previous points. - Only one category of sexual crimes. - Based on sample a crime records. - Some records may have contained recording errors (e.g. using an incorrect crime code). - Produces estimates and the true value may differ slightly from the findings due to sampling error. As such, analysis is a broad indication rather than an exact measure.
Her Majesty's Inspectorate of Constabulary (HMICS) Crime Audit	- Audit of crime recording by Police Scotland to assess compliance with Scottish Crime Recording Standard (SCRS) and counting rules. - Examined over 6,000 incidents and 5,000 crimes.	- Doesn't include all crime types. - Mainly for operational purposes rather than analytical. - The records included are only

	• Examined records in five categories: sexual crime; violence; damage; non-crime related incidents; and no-crimes. • A proportionate, random sample for each of the five categories was selected in 13 local policing divisions. • Reported results are statistically significant with Scotland-wide confidence intervals at the 95% level	a sample of the total population and are subject to sampling error.
Police Recorded Crime in England and Wales	• Statistics on crimes that are recorded by the police derived from administrative police records. • Collected by the Home Office • Covers the full range of crimes and offences. • Data published by crime classifications. • Since April 2015 police forces have been required to return information on the number of crimes flagged as being committed online (full or in part). • Provides whole counts rather than estimates.	• See points on Police Recorded Crime in Scotland. • Trends etc., will not necessarily be directly applicable to Scotland. • Difference in crime recording systems and crime/offence classifications in England and Wales than in Scotland.
Scottish Household Survey (SHS)	• Annual large scale representative social survey. • Includes a nationally representative sample of 10,500 households, 9,600 adults in private residencies. • Survey carried out via face-to-face questionnaire. • Covers a range of topics and provides weighted estimates.	• Does not include those living out-with private residencies. • Data from a sample of the population so subject to sampling error.
Scottish Public Opinion Monitor 2016	• Telephone survey of 1,000 adults in Scotland aged 18+. • Fieldwork carried out 6-13 June 2016. • Weighted data. • Scottish Government funded a module on cyber-crime.	• Does not provide population prevalence rates. • Is not quality assured (like the SCJS and CSEW) to ensure experiences amount to criminal incidents. • Sample size does not allow for detailed breakdowns. • Subject to sampling error.
Cyber Security Tracker 2017	• UK panel survey which includes 1,057 individuals in Scotland, UK sample 4,052. • Fieldwork carried out 7 Feb-6 Mar 2017.	• For marketing purposes primarily. • Representativeness of sample unclear. • Subject to sampling error.
Scottish Schools Adolescent Lifestyle and Substance Use Survey (SALSUS)	• Self-completion survey administered by teachers under exam conditions. • A random nationally representative sample of S2 and S4 pupils (13 and 15 year olds) in school was selected with classes as the primary sampling unit. • Data weighted by local authority, age, sex,	• Excludes pupils in special schools, secure residential units and those who are home schooled. • Data from a sample of the population so subject to sampling error.

	school sector (state/independent), school denomination and by urban/rural classification. • 2015 survey, 25,304 pupils participated. • Conducted on a biennial basis.	• Concerns about the honesty of responses especially given the sensitive topics covered.

Context

Whilst the growth of the internet and cyber technologies has created many positive opportunities, these are accompanied by inherent risks and the potential to be exploited by criminals. This section sets the review’s findings in context by exploring the levels and trends in internet use across Scotland.

Internet use

The vast majority of adults (84%) reported using the internet for personal or work use in 2016[13]. The figure has remained steady of late but has markedly increased since the 2007 baseline of 63%. There is a clear relationship between internet use and age, with the percentage of adults using the internet increasing as age decreases. Generally speaking internet use increases as household income rises.

Almost all adults (97%) who use the internet for personal use do so at home. However the ways in which people access the internet for personal use are becoming increasingly diverse. Access on the move via a mobile phone or tablet rose by six percentage points over the year to 51%[14] in 2016, with higher earning households being more likely.

Security measures

There are indications that the public are aware of the potential risks of using the internet, with the majority taking precautions to protect themselves. In 2016 68% of adult internet users in Scotland said they don’t open emails or attachments from unknown senders, 67% avoid giving personal information online and 64% use different passwords for different accounts. However some security measures are more commonly used than others.

Only 7% of internet users adopt none of the security measures asked about. Use of security measures varies by age and area deprivation, with older users and those living in the 20% most deprived areas less likely to employ such measures. The public’s online behaviour and preventative action plays a crucial role in minimising the risks of negative online encounters.

[13] Scottish Household Survey, 2016

[14] Asked of adults who use the internet for personal purposes

Group 1 – Non-sexual crimes of violence

Summary of findings

- The available evidence suggests that cyber technology appears to be having no significant influence on the scale or nature of non-sexual crimes of violence.
- There is insufficient evidence to assess the role of cyber technologies in cases of threats and extortion in Scotland.

Violent crime

Non-sexual crimes of violence are typically contact related incidents, so by definition we might expect to find that technology does not play a particularly prominent role. Where technology may play a part is in the stages which lead up to the occurrence of violent incidents e.g. used by offenders to make contact with victims.

Scottish police recorded crime data shows non-sexual crimes of violence accounted for 3% of all crimes recorded in Scotland in 2016-17. Between 2002/03 and 2014/15 levels decreased, before rising in 2015-16 and 2016/17. The most recent increase marked a 6% change from 6,737 crimes in 2015/16 to 7,164 in 2016/17. In spite of this increase, the recording of these crimes fell by 44% between 2007/08 and 2016/17. It is not currently possible to identify cyber incidents, however the below evidence from England and Wales would suggest that that the number is likely to be low.

The Scottish Crime and Justice Survey (SCJS) does include data on where incidents of valid[15] violent crime occurred. Yet given the general nature of violent crime, it is perhaps unsurprising that in recent sweeps no incidents have been noted as occurring 'online/via the internet.' Part of this could be attributable to the sort of violence captured by the SCJS, which tends to be more physical in nature, for instance threats are not counted as crimes. In addition any incidents would have to occur solely online to illicit this response, meaning incidents where the internet was involved but the crime itself occurred elsewhere would not be included.

A similar finding is also apparent in the Crime Survey for England and Wales (CSEW). The latest findings (year ending September 2016) from their 'cyber flag' approach (allows for the coding of 'traditional crimes' that are cyber-related), found that 0.2% of violent incidents were identified as a cyber-crime[16].

[15] Valid crimes are those which occurred in Scotland, during the reference period and concern crimes that are within the scope of the SCJS. Any incident that does meet any of these criteria is invalid.

[16] Crime in England and Wales, Year ending September 2016.

Since April 2015 it is mandatory for police forces in England and Wales to return information on the number of crimes flagged as being committed online (full or in part). The latest experimental statistics reveal that for the year ending September 2017, only 0.2% of all 'other violence against the person' offences[17] were noted as having an 'online-element' (full or in part)[18]. This is unchanged from the previous year.

Overall, the limited available Scottish data and the emerging data from elsewhere would suggest that violent crime continues to have no obvious or significant online element.

Future evidence on violent crime

Looking to future evidence, a 'cyber flag' question is being added to the victim form section of the SCJS questionnaire from April 2018. Amongst other crimes, this will provide data on the proportion of violent crimes (includes serious assault, minor assault and robbery) that have a cyber-element, and as trend data is gathered, allow us to analyse how this is changing over time.

Police Scotland introduced a cyber-marker to their crime recording systems in April 2016. Police Scotland are currently considering how to enhance how crimes with a cyber-element are marked.

Threats and Extortion

In this group we also find threats and extortion[19]. There is very little known evidence in relation to extortion as a whole (obtaining money or any other advantage by threats). Police recorded crime statistics for Scotland show there was 425 cases of threats and extortion (as a whole) in 2016/17. This is a 25% increase from 2015-16[20] but the numbers remain small. Whilst some individuals may experience cyber-related extortion, it is likely that the experiences and incidents captured by existing data sources are often reported in relation to other crimes (for instance computer misuse or sexual crime).

The Abusive Behaviour and Sexual Harm (Scotland) Act 2016 introduced new offences covering the threat to disclose or disclosure of an intimate image with the offences coming into force in July 2017, with the majority of crimes relating to the new legislation likely to have a cyber element. Previously, if there is an element of gain of a sexual nature, on the part of the perpetrator from threatening to disclose the image, a crime of attempted extortion/extortion may be recorded. This would

[17] Crime in England and Wales, Year ending September 2017, Experimental tables, Police Recorded Crime

[18] The experimental data on the extent of cyber-related crime is derived from a 'flag' recently added to recorded crime records, so the quality of the data is still under review and may be improved in due course. The figures should therefore be interpreted with caution.

[19] Incidents of threats and extortion are also discussed in the section on Group 6 offences which encompasses 'threatening and abusive behaviour.

[20] Recorded Crime in Scotland, 2016-17

now be recorded as a sexual crime of ‘threatening to disclose an intimate image’. Furthermore, some disclosure of intimate material previously recorded as a Communications Act 2003 offence (Group 6 - Miscellaneous Offences) would be recorded as a sexual crime of ‘disclosure of an intimate image’. It is likely that the introduction of this legislation will lead to the transfer of some existing activity into Group 2 - Sexual Crime (most likely from Group 1 - Non-sexual violent crime and Group 6 - Miscellaneous Offences) as well as some additional activity newly recorded within Group 2. It should also be noted that any sexual activity a person is coerced into as a result of being threatened with the disclosure of an intimate image would still be recorded as a further sexual crime.

Group 2 – Sexual crimes

Summary of findings

- Cyber technology has had an impact on both the scale and nature of sexual crime in Scotland.
- Estimated that the internet was used as a means to commit at least 20% of all sexual crimes recorded by the police in 2016/17.
- Online sexual crimes tend to be concentrated around non-contact offending but the internet may be a precursor in contact sexual crimes e.g. rape, sexual assault.
- The number and proportion of police recorded 'other sexual crimes' in Scotland which were cyber enabled (the internet used as a means to commit the crime) has increased. In 2016/17 51% of 'other sexual crimes' were cyber-enabled, up from 38% in 2013/14.
- Cyber enabled 'other sexual crimes' have contributed to the growth in all police recorded sexual crimes in Scotland between 2013/14 and 2016/17.
- When the specific 'other sexual crimes' of 'communicating indecently' and 'cause to view sexual activity or images' are cyber-enabled:
    - Victims and offenders tend to be younger, with the majority of victims aged under 16.
    - Victims and offenders are more likely to know of one another.

Sexual crimes

Published literature and media reports often suggest one of the main areas where the development of computer technology has created new opportunities for criminal activity is sexual offending. However, sexual crime is a wide-ranging category incorporating both 'contact' (e.g. sexual assault) and 'non-contact' (e.g. possession of indecent images) offending, meaning that the role technology could potentially play is complex[21].

SCJS findings suggest the level of sexual crime experienced in Scotland has remained fairly constant over recent years. There were no statistically significant differences in the prevalence of adults experiencing serious sexual assault (e.g. rape) or 'less serious' sexual offences (e.g. indecent exposure) between 2008/09 and 2014/15[22].

The latest police recorded crime figures show sexual crime increased by 65% between 2007/08 and 2016/17, and 5% between 2015/16 and 2016/17[23].The

[21] For instance, whilst someone obtaining illicit images of children via the internet would certainly be considered a cyber-crime, it is somewhat more challenging to assess the role of technology in facilitating 'contact' crimes between people who initially meet online, through a dating website for example.

[22] Scottish Crime and Justice Survey, 2014-15.

[23] Recorded Crime in Scotland, 2016-17

biggest increase by far in sexual crimes recorded by the police in Scotland has been in 'other sexual crimes'[24], which have increased by 146% since 2010/11. Almost 63% of the total growth in recorded sexual crime over this time can be attributed to 'other sexual crimes'[25]. The contrasting findings of the two sources suggest that the growth in recorded sexual crime may be in part due to a greater willingness of victims to report incidents to the police and the role of targeted police operations.

Online sexual crimes

An audit of crime recording standards by HM Inspectorate of Constabulary in Scotland (HMICS)[26] in 2016 found just over 10% of the sample of sexual incidents scrutinised (1,117) involved an online element. Children were reportedly the victims in a substantial proportion of these cases, with many involving young children (aged under 13). The audit also found the majority of the cyber-enabled sexual incidents they examined involved social media channels such as Facebook, Twitter, Instagram and Oovoo, as well as online dating sites. Resulting crimes varied including but not limited to rape, communicating indecently and possession of child and extreme pornography.

Whilst the SCJS is the most reliable source of evidence on the prevalence of sexual victimisation in Scotland, the survey has not collected data which enables an assessment of whether sexual crimes involved an online element[27]. In addition, the Police Scotland cyber marker is still being embedded and developed.

In the absence of further Scotland data, we turn to England and Wales. Experimental police recorded crime data for the year ending September 2017[28] shows 0.7% of sexual offences[29] (excl. child sexual offences) and 13% of child sexual offences were flagged as an online, both unchanged from the previous year.

Setting these figures in context, England and Wales recorded crime figures show a larger increase in total sexual offences than in Scotland: 19% increase over the year ending June 2017[30], whilst the 2016-17 annual increase in Scotland amounted to 5%. Looking at longer term trends, the percentage change in England and Wales is also markedly higher than in Scotland. However differences do exist

[24] Includes crimes such as communicating indecently, taking, possessing and distributing indecent photos of children, sexual exposure, public indecency and causing to view sexual images or activity.

[25] Recorded Crime in Scotland: Other Sexual Crimes, 2013-14 and 2016-17

[26] HMICS Crime Audit, 2016

[27] The SCJS does separately gather data on experiences of receiving (repeated) obscene or threatening communications. However such communications may not always involve a sexual component and so the available evidence is discussed in the section on Group 6- Misc. Offences

[28] Crime in England and Wales, Year ending September 2017, Experimental tables, Police Recorded Crime

[29] Includes crimes such as rape, sexual assault, sexual activity without consent, incest, exposure and voyeurism etc.

[30] Crime in England and Wales, Year ending June 2017, Bulletin tables, Police Recorded Crime

between the two jurisdictions in how they measure and record crime, so caution should be taken when comparing these sources[31]. Therefore whilst this is a useful evidence source, it might be assumed that trends in online sexual offences in England and Wales are not necessarily directly applicable to Scotland. It should also be noted that there are large variations in the use of the cyber flag between police forces and anecdotal evidence suggests the flag is being underused.

Online 'other sexual crimes'

As mentioned, the biggest increase in sexual crimes recorded by the police in Scotland has been in 'other sexual crimes'. Many of the crimes in this category do not include any direct physical contact between the victim and the perpetrator(s). As such, it is reasonable to consider that many have the potential to be cyber-enabled (internet used as means to commit the crime).

Scottish Government research involving a sample of police records found a significant increase in the proportion of 'other sexual crimes' that were cyber-enabled[32] from 38% in 2013-14 to 51% in 2016-17[33]. This allowed the research to estimate that the internet was used as a means to commit at least 20% of all sexual crimes recorded by the police in 2016/17.

The rate of 'other sexual crimes' that were cyber-enabled varied according to the specific crime. The three crimes with highest rate of cyber-enabled acts were indecent photos of children (98% cyber in 2016/17), cause to view sexual activity or images (71%) and communicating indecently (58%).

The research estimated that the number of cyber-enabled 'other sexual crimes' doubled between 2013-14 and 2016-17 to 2,224. Comparing this to the estimated growth in 'other sexual crimes' and all sexual crimes, suggests that approx. 77% of the increase in 'other sexual crimes' and 51% of the growth in all sexual crimes during this time is due to growth in cyber-enabled 'other sexual crimes'. Overall therefore, it seems that a sizeable (and increasing) proportion of sexual crimes recorded by the police may have a cyber-element.

Crucially however, there are no (or substantially less) directly comparable figures on 'other sexual crimes' from the SCJS, due to the emphasis within the survey on contact offending. Consequently there is no way of assessing whether the recent increases in such crimes recorded by the police and the percentage that are cyber-enabled is a genuine change or the result of a greater willingness to report and targeted police operations.

Victims and perpetrators of online 'other sexual crimes'

[31] There are differences between the respective Scottish Crime Recording Standard and the National Crime Recording Standard for England and Wales.

[32] Crimes that weren't committed through the internet but involved some form of online communication prior to them occurring aren't classified as cyber enabled crimes. For example where a perpetrator arranges via social media to meet someone, and when they meet in person communicates indecently with them.

[33] Recorded Crime in Scotland: Other Sexual Crimes, 2013-14 and 2016-17.

The Scottish Government research explored two ‘other sexual crimes’ in more detail ‘communicating indecently’ and ‘cause to view sexual activity or images’, in order to see if there were any differences between cases which were and were not cyber-enabled. In 2016/17 these two crimes accounted for:

- Around 60% of cyber-enabled ‘other sexual crimes’;
- more than half of all ‘other sexual crimes’; and
- a fifth of all recorded sexual crimes in Scotland.

Analysis found that where identifiable, there was no statistically significant difference in the gender of victims and perpetrators according to whether or not the crime was cyber-enabled. In 2016/17 for both cyber-enabled and non cyber-crimes of this type, more than 80% of victims were female and around 95% of perpetrators were male. Whilst this suggests cyber technology is not influencing the gender profiles of either victims or perpetrators, it is interesting to note that the proportion of male victims of cyber-enabled crimes of ‘communicating indecently’ and ‘cause to view sexual activity or images’ did significantly increase, from 8% in 2013/14 to 16% in 2016/17.

Online child sexual offences

Continuing with the ‘other sexual crime’ research, analysis of occurrences of ‘communicating indecently’ and ‘cause to view sexual activity or images’ revealed victims and perpetrators tended to be much younger where these crimes were cyber-enabled. This is detailed in Table 2.1.

Table 2.1: Victims and perpetrators 2016/17- ‘Communicating indecently’ and ‘Cause to view sexual activity or images’ (where identifiable, based on cases sampled)[34]

Cyber status	Median age		% under 16 yrs.		% under 20 yrs.	
	Victim	Perpetrator	Victim	Perpetrator	Victim	Perpetrator
Cyber-enabled	14	18	74	26	83	57
Not cyber-enabled	23	36	32	6	42	14

Source: Source: Recorded Crime in Scotland, 2016-17 and ‘Other sexual crimes’ research

Adding another dimension, the research found there to be a higher proportion of cyber-enabled incidents involving both a victim and a perpetrator aged under 16. In 2016/17 24% of cyber-enabled crimes of ‘communicating indecently’ and ‘cause to view sexual activity or images’ fell into this bracket, compared to 8% of non-cyber-enabled crimes.

The relationship between victims and perpetrators also varied depending on whether or not these crimes were cyber-enabled. Victims and perpetrators were more likely to be acquaintances[35] when these crimes were cyber-enabled (47% in 2016/17) than where they were not (26%).

[34] Cyber enabled victim base 405, not cyber enabled victim base 244. Cyber enabled perpetrator base 279, not cyber enabled perpetrator base 209.

[35] May include friends, neighbours, colleagues, class mates, etc.

Perhaps linked to the age profile of cyber-enabled victims and perpetrators, the research found that a mobile phone was the most commonly used device in cases of cyber-enabled 'communicating indecently' and 'cause to view sexual activity or images'. In over 90% of cases, websites or apps were mentioned in 2013/14 and 2016/17. The latter saw a greater variety of apps and websites used, including Snapchat and Instagram but Facebook was still the most commonly mentioned app.

The role played by social media was also reflected in the HMICS 2016 audit, where it was found much sexual harm to children was committed via apps on smartphones and tablets[36]. The audit raised concerns that some of the most popular social media networks used by children are recurring vehicles for sexual crime and that (in many of the cases examined) sexual harm to children was committed via apps on smartphones and tablets which did not have parental controls in place or had been overcome.

Taking the evidence together suggests there is a relationship between recorded 'other sexual crimes' affecting children and cyber technology. This relationship is likely to be complex and influenced by a number of factors, some of which have been touched on including reporting behaviours and the behaviours of perpetrators. But amongst others, targeted police operations[37] and the reporting behaviours of adult victims are also likely to play their part. However, clearly this only captures certain types of sexual offending and perhaps most importantly, only relates to crimes which come to the attention of the police.

Reporting of online sexual crimes

The Scottish Government research found that the most common way the police became aware of the 'other sexual crimes' sampled was by the victim reporting it (39% in 2016/17). However this varied depending on the crime. Looking more specifically at 'indecent photos of children', (where 98% were cyber-enabled), the vast majority (81%) were discovered through police investigation/intelligence (this includes cyber and non-cyber occurrences). Given the nature of this crime, this is perhaps to be expected.

Analysis revealed in 2016/17 cyber-enabled crimes of 'communicating indecently' and 'cause to view sexual activity or images', were less likely to be reported by victims themselves: 34% compared to 65% of crimes that weren't cyber-enabled. Yet, a higher proportion of cyber-enabled crimes were reported by a relative or guardian (38% vs. 11%) and by a responsible person[38] (11% vs. 5%). This likely reflects the age profile of victims where these crimes were cyber-enabled (74% aged under 16), as was discussed above.

[36]Related to recorded cyber-enabled sexual crimes as a whole. HMICS Crime Audit, 2016

[37] For example Operation Latisse, a national initiative focused on tackling online child sexual abuse

[38] A person with some form of professional responsibility towards the people involved in the crime (e.g. a social worker, teacher, or care home staff etc.)

Furthermore, the analysis could also point towards the reporting behaviour of adult victims i.e. some adults may view such behaviour as more of a nuisance rather than a crime warranting of being reported. Whilst there is no evidence to substantiate this line of thought, if found to be true this would suggest that these incidents are occurring more widely in society than the recorded crime figures show.

Future evidence on sexual crime

Since 2016/17 the SCJS has been capturing experiences of ‘revenge porn’, one of the areas of sexual offending which is regularly considered as being associated with the growth of cyber technology. Data will also be available on the emotional response of victims to help us understand the impact of such experiences. This will be available from Spring 2018.

The Growing Up in Scotland longitudinal survey is due to collect information on online experiences of children in their first year of secondary school and parental mediation later in 2017 which will offer a more up-to-date source of evidence on these matters which also will be robust and representative of experiences in Scotland.

Police Scotland introduced a cyber-marker to their crime recording systems in April 2016. Police Scotland are currently considering how to enhance how crimes with a cyber-element are marked. Likewise, work is on-going within police forces in England and Wales to improve the identification of online offences.

ONS are in the process of developing a cyber-crime module for the CSEW 10-15 year old questionnaire. These questions might include elements of sexual crimes. This data will not be available for some time as the questions have yet to be incorporated into the survey.

Group 3 – Crimes of dishonesty

Summary of findings

- Evidence suggests that fraud is one of the most numerous crime types, but this is not entirely driven by the internet.
- SCJS indicative data shows 5% of adults reported that they were victims of bank and credit account fraud in 2014/15, and this has increased in recent years. However the data is subject to caveats.
- Crime Survey for England and Wales (CSEW) data shows 3.2 million incidents of fraud were experienced by 5.9% of adults in the year ending Sept. 2017.
- For the year ending Sept. 2017, the CSEW estimates 56% of fraud incidents were cyber (internet or any type of online activity related to any aspect of the offence), amounting to an estimated 1.8 million incidents.
- As yet no victimisation survey has published data looking at the victims, impacts and reporting of fraud which is committed via the internet. This could reflect methodological challenges.
- Incidents of fraud (as whole) are underreported to Action Fraud and the police. This is likely linked to incidents generally being viewed as having no emotional or physical impact or as an inconvenience (rather than anything more harmful), in addition to the relatively high rates of financial reimbursement.
- There is insufficient CSEW time series data in order to establish any trends in the incidence and nature of fraud, including the role of cyber technology.

Fraud (as a whole)

Fraud can take many (sometimes related) forms, all of which centre around a person dishonestly and deliberately deceiving a victim for personal gain (e.g. using someone else's bank or credit card details to make a purchase). The growth of the internet has offered new means for fraud to be committed and possibly on a larger scale than before. This has led to the common claim that fraud has grown significantly in recent years and may represent the majority of cyber-crime incidents alongside experiences of computer misuse. Before considering fraud occurring online, by way of providing context this review briefly considers the key evidence relating to fraud as whole.

The SCJS has never traditionally measured fraud, but does include questions on people's perceptions and experiences of certain types of fraud (in the form of 'Victim Form Screener' questions). These questions provide indicative findings only because respondents are not asked for full details of the incidents in the way that they are with other traditional SCJS incidents (which enables us to assess whether to code incidents as valid crimes). Furthermore it is not possible to detect whether such incidents occurred online or not.

In relation to bank and credit account fraud, analysis shows the (indicative) victimisation rate has significantly increased in recent years from 3.5% in 2008/09 and 4.1% in 2012/13 to 5% on 2014/15. This finding is similar to the CSEW figures for the year ending September 2017, which estimate 4.3% of adults experienced bank and credit account fraud[39] and, 5.7% of plastic card owners reported they were victims of card fraud[40].

The 2016-17 police recorded crime data shows that fraud[41] accounts for 7% of all ‘crimes of dishonesty’ in Scotland[42]. Despite small fluctuations in the period 2007/08 to 2016/17, cases of fraud decreased by 7%. However looking at the last annual change (2015/16-2016/17) reveals a 6% increase to 7,811 crimes. The level of fraud being brought to the attention of the police in Scotland is clearly much smaller than what we might anticipate based on indicative data from the SCJS and the CSEW findings.

Detailed questions were added to the CSEW in October 2015 to provide greater insight into the extent, nature and impact of fraud. Findings for the year ending September 2017 reveal an estimated 3.2 million incidents[43] of fraud were experienced by 5.9% of adults[44]. Bank and credit account fraud was the most numerous, accounting for 2.3 million incidents. Compared to the previous year (ending September 2016) total incidents of fraud fell by 10%, whilst the prevalence rate was similar. Further time series data is needed before any trends can be established in these and the other CSEW fraud findings.

Earlier CSEW experimental data (year ending March 2017) also provides an insight into the nature of fraud incidents including[45]:

- Fourteen per cent of fraud victims had been victimised more than once (in the same 12 month period).
- Almost three-quarters (73%) of fraud incidents involved an initial loss of money, property or goods[46], irrespective of whether a loss was recovered.

[39] Crime in England and Wales, Year ending September 2017, Additional tables on fraud and computer misuse, CSEW

[40] Overview of fraud and computer misuse statistics for England and Wales. This is an indicative finding.

[41] It is worth noting that this will include crime reported by both individuals and business, as well as both traditional and cyber-related fraud.

[42]Recorded Crime in Scotland, 2016-17

[43] Crime in England and Wales, Year ending September 2017, CSEW

[44] Crime in England and Wales, Year ending September 2017, Additional tables on fraud and computer misuse

[45] Crime in England and Wales: Year ending March 2017, Experimental Tables, CSEW

[46] Financial loss, including money stolen and additional charges or costs incurred, as well as loss of property or goods.

- Victims received a full reimbursement in 75% of fraud incidents where a loss was incurred.
- Sixty-eight per cent of fraud incidents involved money being taken/stolen[47] from the victim (regardless of reimbursement status). In the majority of these incidents (63%), the loss was less than £250.

Another aspect of fraudulent activity concerns the trading of fake goods. Yet there is very limited information available, although in theory the internet offers new avenues for this. However the SCJS has been collecting information on smuggled or fake goods since 2016/17 and this is discussed further in the section on future evidence.

Online fraud

The detailed CSEW questions crucially include a high level cyber 'flag', which allows for the identification of incidents where the internet or any type of online activity was related to the offence. The latest figures (year ending September 2017) reveal 56% of fraud incidents were cyber-crime[48], as shown in Table 3.1. Applying this to the number of fraud incidents (3.2 million), shows there was an estimated 1.8 million incidents during this time. Comparing the first two years' worth of data, shows that the proportion of fraud incidents that are cyber has remained relatively constant over this time and this holds across fraud types, however further time series data is needed to establish a trend.

The proportion marked as cyber did vary according to the specific type of fraud. Of particular note in the CSEW findings is that around half (51%) of bank and credit account fraud incidents were **not** cyber, yet (as mentioned above) incidence numbers estimate this to be the most common type of fraud. Suggesting that while fraud may be numerous, the scale of the issue is not entirely driven by the internet (perhaps in contrast to popular opinion), although it clearly is a factor.

Table 3.1: Proportion and number of fraud incidents* flagged as cyber, CSEW year ending September 2016 and 2017[49]

Offence group	% cyber 2016	Base 2016	Est. no of incidents 2016 (thousands)	% cyber 2017	Base 2017	Est. no of incidents 2017 (thousands)
Fraud	53	1219	1,917	56	1052	1,814
Bank and credit account fraud	45	806	1,103	49	758	1,171
Consumer and retail fraud~	75	342	704	81	262	605

Advance fee fraud and 'other' fraud incidents are not reported as the base is fewer than 50.
~For year ending September 2016 this was categorised as non-investment fraud but was renamed to reflect the corresponding name change to the Home Office Counting Rules from April 2017.

[47] Money stolen or taken as a direct result of fraud or any additional charges or costs incurred (e.g. bank charges etc.).

[48] Cases where the internet or any type of online activity was related to any aspect of the offence.

[49] Crime in England and Wales, Year ending September 2017, Additional tables on fraud and computer misuse

The Office for National Statistics (ONS) recently published CSEW data[50] showing the proportion of adult internet users experiencing negative online incidents, for the year ending March 2011 to year ending March 2017[51]. The proportion experiencing a 'loss of money' has remained fairly constant across the time series, between 2% and 3%. This would appear to chime with the above findings which suggest that fraud still holds a substantial offline dimension. Although this data does only concern one aspect of fraud and is not an indication of wider prevalence. It is important to note that these findings do not necessarily relate to criminal activity and some incidents would not be classified as crimes.

Subject to the same caveats, the 2016 Scottish Public Opinion Monitor found that in the previous 12 months, 5% of adult internet users[52] (aged 18 and over) had experienced financial loss due to fraudulent payment card and 3% had lost money as a result of receiving fraudulent messages.

Impacts of fraud

As part of their experimental statistics series, ONS published CSEW analysis on the emotional and physical impacts of all fraud incidents for the year ending September 2016. Unfortunately, they have not yet been able to split this into online and offline fraud, but analysis shows that 9% of all fraud incidents resulted in people 'no longer using specific websites[53]. This would suggest that such websites played a part in the fraud incident and/or these incidents raised awareness of online risks more broadly, prompting this action. This behaviour was most common amongst fraud incidents which resulted in a loss of money/goods/property that was only partially recovered or not at all (15%). These findings are perhaps useful for understanding the motivations and drivers behind some online security behaviours, and possibly gives us an indication of the types of frauds being experienced online.

Looking at the impacts of fraud as a whole, in around half of incidents (49%), victims identified no emotional or physical impacts but this fell to 23% for incidents involving a loss that was only partially reimbursed or not at all. Just over a fifth (22%) of incidents resulted in a 'loss of time/inconvenience', the most commonly cited impact . However in fraud incidents with a loss which was only partially reimbursed or not at all, the most commonly experienced impact was 'felt ashamed, embarrassed, self-blame or similar'. These emotions occurred in 25% of such incidents, compared to 4% of incidents where the loss was fully reimbursed. Suggesting that being able to recover money was a determinant in preventing or triggering these sorts of emotional responses. Such responses could also impact on the likelihood of people reporting incidents to the police.

[50] In response to an ad hoc request

[51] Proportion of adult internet users experiencing negative online incidents, year ending March 2011 to year ending March 2017

[52] Scottish Public Opinion Monitor June 2016. Question base 862.

[53] Emotional and physical impact of incidents of fraud, by loss (of property or money), year ending September 2016 CSEW (Experimental Statistics)

Victims of fraud

SCJS indicative data shows that in general, the risk of experiencing bank and credit account fraud in 2014/15 was fairly evenly distributed across the population, however some groups were statistically more likely to report experiencing this type of fraud than others:

- Those aged 25-44 (6%) and 45-59 years (6%) were more likely than adults aged 60 plus (3%).
- Adults in managerial and professional occupations (8%) compared to those who have never worked or are long-term unemployed (3%).
- Households situated out-with the 15% most deprived areas in Scotland (5%), compared to those within the 15% most deprived (3%).

Some of these differences are also apparent in the CSEW fraud statistics for the year ending March 2017, although the two are not measuring like-for-like. CSEW data[54] shows that again, generally speaking, experiences of fraud (on and offline) appear to be more evenly spread amongst the population than other types of crime. That said, some personal and household characteristics do appear to be associated with being a victim of fraud and those with the higher risk of victimisation often differ from other crime types:

- Fraud victimisation is higher in the middle of the age distribution: adults aged 35-44 are more likely to be a victim of fraud (7.4%) than 16-24 year olds (4.9%). This differs from violent crime and most property crime types where the youngest age group is at higher risk of being a victim.
- Households with an income of £50,000 plus are more likely to be a victim of fraud (8.8%). This compares to 5.3% of households with an income of less than £10,000 and is unlike crimes of violence.
- Individuals in managerial and professional occupations are more likely to be a victim of fraud (8.0%) than full-time students (4.6%). This is in contrast to violence and burglary where student households are amongst those at greatest risk.
- Individuals living in the 20% least deprived areas[55] are more likely to be a victim of fraud (7.2%) than those living in the 20% most deprived (5.3%). This is the opposite from a number of other crimes.

Overall, this suggests that fraud is not only more prevalent than other crime types[56] but exhibits different patterns too (although the former may be partly as a result of the latter). Caution should be taken when looking at the above characteristics in isolation as some are likely to be closely associated with each other.

[54] Crime in England and Wales, Year ending March 2017, Experimental tables, CSEW

[55] English Indices of Deprivation

[56] For example, for the year ending March 2017, 1.6% of adults were victims of violence and 0.2% were victims of robbery. There were around 1.2 million incidents of violence and 142,000 robberies.

Reporting of fraud

As noted earlier, comparing police recorded crime data in Scotland to findings from victimisation surveys suggests incidents of fraud are underreported. The level of fraud (7,811 crimes) being brought to the attention of the police in Scotland is clearly much smaller than what we might anticipate based on indicative data from the SCJS and the CSEW findings.

Turning to England and Wales, CSEW data for the year ending September 2016 shows 12% of fraud incidents were reported to Action Fraud[57] and this is similar across fraud types[58]. The main reason why fraud incidents aren't reported would appear to be a lack of awareness of the organisation, cited in 66% of incidents. A further 15% weren't reported because victims believed they would be reported by another authority. Taking this together with fact that most losses are reimbursed, we might expect that it is quite a common response for incidents to be reported to a victim's bank or other relevant authority (e.g. building society, credit card company), suggesting that recovering losses is the primary interest of victims (where a loss is incurred). At present however, no data is available to substantiate these assumptions.

Whilst there is no agreement in place between Action Fraud and Police Scotland, it may be reasonable to assume that these reasons for non-reporting, with the exception of a lack of awareness of Action Fraud, feature in why incidents are underreported to the police in Scotland.

Future evidence on fraud

Questions on people's experiences of a range of negative and harmful online activities will be included in the 2018/19 SCJS questionnaire, including identity theft, online dating fraud and incidents of scam emails. Findings from these questions signify an important first step towards developing the evidence base, but they will not be included in main SCJS incidence or prevalence estimates. Indicative data will be available in late 2019/early 2020.[59]

As mentioned earlier, the SCJS has been collecting information on smuggled or fake goods[60] since 2016/17. This includes whether anyone has offered to sell respondents specific types of goods[61]and where this took place, for which 'on the internet' is an option. This data will be available in Spring 2018.

[57] Action Fraud is the national recording centre for fraud offences in England, Wales and Northern Ireland, that were previously recorded by individual police forces. Individuals and businesses are advised to report any incidents directly to Action Fraud. Cases are passed onto the National Fraud Intelligence Bureau (NFIB).

[58] Crime in England and Wales, Year ending September 2016, Experimental tables, CSEW

[59] This will not provide estimates about the extent of online fraud or victimisation and will not be included in main SCJS incidence or prevalence estimates.

[60] Part of quarter sample module.

[61] Cigarettes/tobacco, alcohol, DVDs/video games, jewellery, clothes, accessories, electrical goods, children's toys and something else.

Police Scotland introduced a cyber-marker to their crime recording systems in April 2016. Police Scotland are currently considering how to enhance how crimes with a cyber-element are marked.

Going forward, there is potential to replicate the detailed CSEW fraud questions in the SCJS but doing so would require a significant amount of other content to be removed from the survey to make space. Whilst in principle this data might be helpful and insightful, we should also consider whether this is a priority evidence gap. The release of additional time series data for the CSEW fraud module, will allow for change over time analysis, including establishing any trends.

Group 4 – Fire-raising, vandalism etc.

Summary of findings

- Whilst available evidence shows computer misuse to be numerous and fundamentally driven by the growth of cyber technology and the internet, in quite a lot of cases the resulting impacts tend to be of low severity.
- The most robust and comprehensive evidence on computer misuse is data gathered via the Crime Survey for England and Wales (CSEW), which incorporates incidents of unauthorised access to personal information (including hacking) and computer viruses.
- CSEW evidence shows 1.5 million incidents of computer misuse were experienced by 2.6% of adults over the year ending Sept. 2017.
- Almost all (97%) incidents were cyber (internet or any type of online activity related to any aspect of the offence) for the year ending Sept. 2017, amounting to an estimated 1.46 million incidents.
- In general, the risks of being a victim of computer misuse are spread fairly evenly across society although some groups are at greater risk than others including higher income households. This is likely linked to the profile of internet users- internet use tends to increase with household income.
- CSEW evidence shows that in 49% of computer misuse incidents victims identified no resulting emotional or physical impacts and by far the most common impact was a 'loss of time/inconvenience', experienced in 31% of incidents (year ending March 2017)[1].
- Police recorded crime data for Scotland suggests that incidents of computer misuse are underreported. In 2016/17 only 30 incidents were recorded under the Computer Misuse Act 1990.

Computer misuse

The term 'computer misuse' is used to capture a number of crimes generally covered by the Computer Misuse Act 1990 (which sits within the Group 4 category for statistical purposes). Activities grouped under the computer misuse label mainly centre around unauthorised access to and (sometimes subsequent) attacks on computer systems, networks and data held – for example hacking and Distributed Denial of Service (DDOS) attacks.

Whilst computer misuse can in some circumstances occur 'offline', the central role of computers and technology in such incidents (as targets as well as means to carry out crime) means we might expect a lot of computer misuse to be cyber-related, hence the reason some define such activity as 'cyber-dependent' crime (as described in the introduction and glossary). However as noted previously, computer misuse incidents may often be related to (or indeed facilitate) further criminal activity.

Recorded crime data reveals that very few incidents of computer misuse appear to come to the attention of the police. In 2016/17, only 30 incidents were recorded by the police in Scotland under the Computer Misuse Act 1990 (causing damage[62]), and a further 17 cases were recorded in connection to unauthorised access to computer material only[63]. The latter of these is classified as Group 6 'Miscellaneous offences' but has been included here for ease.

Looking at 'causing damage' in more detail, recorded crime figures show that the number of cases doubled from 9 in 2013/14 to 18 in 2014/15, before increasing to 31 in 2015/16. It would seem unlikely the number of cases in Scotland are as small as these figures suggest, pointing to under reporting, although there is currently limited information available to enable us to unpack why this might be.

The most reliable evidence on computer misuse is the data gathered through the CSEW module added in October 2015. The Office for National Statistics (ONS) report on computer misuse as a whole, computer virus[64] and unauthorised access to personal information (including hacking). For the year ending September 2017, the CSEW estimated there were 1.5 million computer misuse incidents. Computer viruses made up the majority of this group (962,000 incidents), with the remainder (541,000) constituting unauthorised access to personal information[65].

Turning to prevalence rates, 2.6% of the adult population were a victim of computer misuse during the year ending September 2017, with 1.7% experiencing a computer virus and 1.0% suffering from unauthorised access to personal information. When comparing to other CSEW crimes, the findings suggest computer misuse is one of the more common types of crime experienced (as measured by the CSEW)[66].

January 2018 saw the release of the first year-on-year comparisons for the CSEW computer misuse questions. Analysis shows the number of computer misuse incidents for the year ending September 2017 fell by 24% on the year ending September 2016, driven by a fall in computer viruses[67]. However this fall was not accompanied by a fall in prevalence rates, which remained statistically unchanged. Whilst this data provides an interesting first insight, further time series data is needed before any trends can be established.

An estimated 16% of computer misuse incidents in the year ending September 2017 resulted in an initial loss to the victim, all of which occurred through computer

[62] Any unauthorised act in relation to a computer which causes material damage (e.g. disruption of communication, supply of money etc.).

[63] Computer Misuse Act 1990

[64] Includes any computer virus, malware or Distributed Denial of Service (DDoS) attack

[65] Crime in England and Wales, Year ending September 2017, Additional tables on fraud and cyber-crime.

[66] For example, for the year ending September 2017, 1.6% of adults were victims of violence and 0.2% were victims of robbery. There were around 1.2 million incidents of violence and 142,000 robberies.

[67] Crime in England and Wales, Year ending September 2017.

viruses. Such losses are mainly associated with additional charges or costs incurred as a result of the virus (e.g. repair/replacement costs). Given the nature of these losses, it is perhaps unsurprising that almost every incident (98%) resulted in no or only a partial reimbursement[68].

In response to an ad-hoc request ONS released experimental time series statistics on negative online incidents between 2010/11-2016/17[69]. Of the incidents asked about, a computer virus was the most commonly experienced amongst adult internet users. In 2016/17 16% reported they had encountered a computer virus. However the proportion has decreased from 33% in 2010/11 and 19% in 2015/16. In comparison, the figure for ‘unauthorised access to/use of personal information’, has remained steady at around 6% over the last year years and this is the same as recorded in 2010/11. It is important to note that these findings do not necessarily relate to criminal activity and some incidents would not be classified as crimes.

Returning to the year ending September 2017 computer misuse data, the CSEW found that the vast majority (97%) of computer misuse incidents could be described as a cyber-crime[70], providing weight to assertions about the centrality of IT to computer misuse crimes. This rate is unchanged from the previous year. Applying this to the total number of computer misuse incidents (1.5 million) shows an estimated 1.46 million were flagged as being a cyber-crime. Perhaps unsurprisingly, it seems possible that computer misuse is one of the crimes which is most fundamentally driven by the growth of the internet (regardless of the scale overall).

A source of Scotland specific data, the Scottish Public Opinion Monitor, found that 14% of respondents who use the internet had experienced a computer virus or other type of infection in the previous 12 months[71]. This was the second most commonly cited experience (of those included). Other computer misuse incidents were unauthorised access to/use of personal data (experienced by 7%) and Ransomware[72] (2%). However the marked difference between these figures and those from the CSEW is likely due to key methodological variations[73], (namely that some incidents reported in the Scottish Public Opinion Monitor may not amount criminal acts per se) rather than such incidents necessarily being much more common in Scotland. Therefore the two are not directly comparable.

[68] Crime in England and Wales, Year ending September 2017, Additional tables on fraud and cyber-crime.

[69] Proportion of adult internet users experiencing negative online incidents, year ending March 2011 to year ending March 2017, CSEW

[70] Cases where the internet or any type of online activity was related to any aspect of the offence.

[71] Scottish Public Opinion Monitor June 2016. Question base 862.

[72] Malicious software that threatens to publish the victim's data or perpetually block access to it unless a money is paid.

[73] Please see sources table on for methodological details.

Victims and impacts of computer misuse

As with the CSEW statistics on fraud, further analysis on computer misuse is not split into cyber and non-cyber incidents, however this is less of an issue here given the very high rate of incidents identified as being a cyber-crime.

Data for the year ending March 2017 shows that almost a fifth (18%) of computer misuse victims, were victimised more than once in the same 12 month period[74]. Generally speaking, the likelihood of being a victim of computer misuse is fairly evenly spread across the adult population. That said, there are a few groups who would appear to be more at risk than others (differences are statistically significant):

- 16-24 year olds (3.5%) than those aged 75 and over (0.9%).
- Adults in employment (3.2%) than those who are economically inactive (2.4%).
- Adults in managerial and professional occupations (4%) than those who have never worked or are long-term unemployed (2%).
- Adults with Apprenticeship or A/AS level qualifications (3.9%) compared to adults with no qualifications (1.2%).
- Households with an income of £50,000 and over (4.4%) than households with an income of less than £10,000 (2.5%).
- Households living in the private rented sector (3.3%) than households in the social rented sector (2.3%).

As was noted in relation to fraud some of these characteristics will likely be closely associated with each other and so caution should be exercised.

Similar to fraud in 49% of computer misuse incidents, victims identified no emotional or physical impacts and this was the same for computer viruses and unauthorised access. By far the most common impact arising was a ‘loss of time/inconvenience’, which was experienced in 31% of incidents (year ending March 2017)[75]. This also held for computer viruses (34%) and unauthorised personal information (26%). This was followed by ‘stopped using specific internet sites’, a consequence in 8% of all computer misuse incidents, suggesting a minority of incidents triggered a change in online behaviour.

Reporting of computer misuse

As noted, it would seem unlikely that the number of cases in Scotland is as small as the recorded crime figures referenced earlier. This points to computer misuse incidents generally not being reported to the police.

[74] Crime in England and Wales, Year ending March 2017, Experimental tables, CSEW.

[75] Emotional and physical impact on victims of incidents of computer misuse, Year ending March 2017, CSEW

Available data reveals that a smaller proportion of computer misuse incidents in England and Wales for the year ending September 2016 were reported to Action Fraud than fraud incidents: 2% compared to 12% respectively[76]. However this may be a reflection on the nature of the offences and of the perceived remit of Action Fraud, even though the organisation is also the national reporting centre for cyber-crime. Looking at reasons for not reporting, the most commonly cited was ‘never heard of Action Fraud’ (66% of incidents), followed by ‘too trivial or not worth reporting’ (12% of incidents). The latter of these is perhaps to be expected given the most frequently cited impact was ‘loss of time/inconvenience’ as opposed to more harmful consequences. Although, the severity of impacts will be relative to each individual victim.

Similarly to the corresponding section on fraud, we could assume that some of these reasons (apart from awareness of Action Fraud), may also feature in why incidents are underreported to the police in Scotland.

Future evidence on computer misuse

The new cyber questions added to the SCJS from 2018/19 include incidents where people had their device infected with a computer virus and where they were locked out of their device until a payment was made (Ransomware). The first indicative findings will be available in late 2019/early 2020[77]. The release of additional CSEW time series data will allow for change over time analysis, including establishing any trends in computer misuse incidents.

[76] Crime in England and Wales, Year ending September 2016, Experimental Tables, CSEW.

[77] This will not provide estimates about the extent of computer misuse incidents or victimisation and will not be included in main SCJS incidence or prevalence estimates.

Group 5 – Other crimes

Summary of findings

- Available evidence suggests the vast majoirty of illict drug users are still sourcing drugs via traditional means, with a a very small proportion obtaining drugs online.
- Concerns that increases in the amount and accessibility of information online would raise the likelihood of contempt of court issues (e.g. jurors finding out information about a case), have yet to be borne out.

Sale of drugs online

Despite concerns about the increased opportunities to buy illicit substances online, the SCJS in 2014/15 found that only 0.6% of adults who had used drugs in the last month sourced their most frequently used substance online[78]. This compares to 35.1% who got the drug from 'someone well known outside their family', 17.0% who bought from a known dealer and a further 13.1% who bought the drug from a dealer not known to them.

Whilst the SCJS methodology means that this is unlikely to include those with the most problematic drugs use and does not include children, it does suggest that "traditional" methods of sourcing drugs are still the most common. The data also focuses on the most recent substance obtained, whereas asking if people have ever bought drugs online could result in alternative findings. Furthermore, communication via the internet, email etc., could be used in the purchasing of drugs from traditional sources e.g. making contact with a dealer, but this would not be captured by the SCJS.

A research project undertaken by Scottish Government analysts looked at police crime records for drug seizure incidents, including where the drugs had been sourced from (where information available)[79]. Findings suggest that the internet does not tend to be a common feature, but as with the above, this may be because the information is not being recorded rather than the internet not being involved.

The Scottish Schools Adolescent Lifestyle and Substance Use Survey (SALSUS)[80] captures experiences of drug use amongst 13 and 15 year olds. The most recent survey in 2015 found that amongst both age groups, children who had used drugs most commonly sourced them from a friend (41% of 15 year olds had obtained the substance from a friend their own age). By contrast, only 1% in each age group said they had sourced their most recently used drugs through a website. Moreover,

[78] Scottish Crime and Justice Survey 2014/15: Drug use.

Question contained within self-completion module of SCJS questionnaire.

[79] Drug Seizures and Offender Characteristics, 2014-15 and 2015-16

[80] SALSUS, Drug Summary Report. Fieldwork Sept 15- Jan 16. 25,304 pupils participated.

the survey found no changes in how drugs were sourced between 2013 and 2015. Suggesting ‘traditional’ methods for sourcing illicit substances still dominate.

Future evidence on the sale of drugs online

The 2016/17 SCJS will provide data on where adults who have ever taken new psychoactive substances sourced their drugs, enabling us to assess whether people are more likely to buy these substances over the internet than other “traditional” drugs. The SCJS is also collecting data on whether and where respondents have been offered smuggled or fake medicines and pills, including online. Data will be available in Spring 2018. Whilst these may not necessarily be illicit substances (or respondents may not know), it does provide a complimentary source of evidence on the availability of such substances online.

Crimes against public justice

Theoretical papers and media articles have highlighted that the increase in the amount and accessibility of information online means that there is increased scope for contempt of court issues to arise. In short, it is claimed that there are now risks that jurors (and others) are able to access details about a criminal incident and those involved, which could influence the outcome of cases and amount to contempt of court. Whilst such actions might be committed by many people unwittingly, equally the potential to do so can be exploited by criminals in order to undermine the criminal justice system with potentially significant consequences. Irrespective of whether intentional or not, such actions could be seen as a challenge to the values on which the justice system is based.

Although this point has been raised by Scotland’s previous Lord Advocate[81] as well as being exemplified by a small number of high profile cases in the media from the UK and elsewhere, it is not reflected in the recorded crime data which shows that in 2016/17 there was only 3 incidents of contempt of court in Scotland, the joint lowest figure over the last 10 years. The figure has hovered around 5 incidents per year since 2012/13[82]. However it should be acknowledged that it is very challenging to police these sorts of incidents.

Given the increasing amounts of information about individuals being placed online (for example with the increasing expansion of social media and social networks), this may be a matter which grows in prominence in years to come. However this will pose its own challenges around how incidents of this nature are identified and captured in reporting.

[81] Tom Perterkin, Call for Contempt of Court review in internet age’, *The Scotsman* (February 22 2015)

[82] Police Recorded Crime, in-house analysis

Group 6 – Miscellaneous offences

Summary of findings

- Available evidence suggests that the internet may commonly feature in cases of stalking and harassment, whilst being pestered, intimidated or insulted in-person is much more prevlanet than experiences carried out via electronic means.
- SCJS evidence indicates that of the 9% of adults ‘insulted, pestered or intimidated’ in Scotland in 2014/15, the vast majoitty (82%) experienced this in-person.
- SCJS evidence shows that in 2014/15, the most common type of stalking and harassment (arguably more serious than the above) was threatening/obscene texts or emails, experienced by 45% of adults who had encountered at least one form of stalking/harassment in the 12 months prior to interview (6.4%).
- Evidence suggests incidents of harassment and threatening/abusive behaviour are underreported to the police, with many viewing it as ‘too trivial’.

Threatening and abusive behaviour

There are claims that the relative ease with which people can make contact with both known and unknown individuals using the internet and the apparent lack of recourse (either in-person or verbally) increases the risk of experiencing threatening and abusive behaviour. For example, Sheridan and Grant suggest that the internet may be 'particularly attractive to would-be harassers', given the 'relative anonymity, the lack of social status cues, and opportunities for disinhibited behaviour' can promote 'greater risk-taking and asocial behaviour'.[83]

Whilst threatening and abusive behaviour can take numerous forms and may not often amount to criminal acts, the SCJS offers the most robust insight into such experiences by asking whether people have been insulted, pestered or intimidated[84] in person or by various other means. In 2014/15, it found that 9% of adults had experienced such behaviour in the previous 12 months, unchanged from 2012/13[85]. The vast majority (82%) had experienced this in-person whilst experiences over electronic forms of communication were much less frequent. For example 8% said they had been insulted, pestered or intimidated in writing via the internet (such as a social networking site), again this was not statistically different

[83] Sheridan, L.P., and Grant, T.D. (2007) 'Is cyberstalking different?', Psychology, Crime & Law, vol. 13, 6, pp. 627- 640.

[84] By anybody who is not a member of their household.

[85] Scottish Crime and Justice Survey 2014/15: Quarter Sample Module Tables.

from the 2012/13 finding. Whilst 6% of those insulted, pestered or intimidated in the last 12 months, had encountered such experiences by text or email.

The 2016 Scottish Public Opinion Monitor[86] found that 4% of adult internet users had experienced abuse/threatening behaviour in the last 12 months when using the internet. In addition, 7% had been exposed to upsetting and/or illegal images. However not all of these experiences will necessarily amount to criminal acts.

Stalking and harassment

The SCJS also separately collects data[87] on arguably more severe examples of stalking and harassment (which are more likely to amount to criminal acts). In 2014/15 6.4% of the adult population had experienced at least one form of stalking/harassment (as defined by the SCJS[88]) and the most common types involved indirect contact[89]. For example 2.9% of the adult population reported obscene or threatening contact by email or text and 1.4% experienced such issues via social network sites. Neither of these 'cyber-stalking' or 'cyber harassment[90]' measures showed any change from 2012/13, the only time series data available.

Looking at the distribution of different types of stalking and harassment amongst those who had experienced at least one form in the last 12 months, the 2014/15 SCJS found the most common type was by threatening/obscene texts or emails (45.0%). Just over a fifth (21.9%) were subject to obscene or threatening approaches on social network sites. This compares to 32.7% who had silent, threatening or obscene phone calls and 15.7% who had someone wait outside their home or work– suggesting electronic forms of contact are more commonly experienced features of stalking or harassment incidents. Findings were consistent with 2012/13 results.

In general, the reporting of harassment and stalking to the police is fairly low when compared to other crimes included in the SCJS.[91] Less than one in five (18.9%) said the police came to know about the most recent incident. The most common reasons for not reporting were that the matter was 'too trivial' (39.1%) or that

[86] Scottish Public Opinion Monitor June 2016. Question base 862.

[87] Via a self-completion module in the SCJS questionnaire.

[88] Respondents are asked if they've experienced any six behaviours more than once: sent unwanted obscene or threatening cards/letters; sent unwanted obscene or threatening texts or emails; unwanted obscene or threatening approaches on social media; obscene, threatening, nuisance or silent calls; being followed or watched; and having someone wait outside their home or work.

Each of can be viewed as a form of stalking and harassment. However, the data do not show whether respondents themselves viewed their experiences as stalking or harassment.

[89] SCJS 2014/15: Sexual Victimisation and Stalking

[90] Cyberstalking: A course of action (more than one incident), perpetuated through electronic means, which causes stress or alarm.

Cyber harassment: Intimidation, repeated or otherwise, through electronic means.

[91] SCJS 2014/15- 38% of crimes reported to the police. Estimated reporting rates ranged from 28% for 'other household theft' (including bicycle theft) to 62% for housebreaking. 44% of violent crime in the main SCJS survey was reported to the police.

victims dealt with the matter themselves (27.0%). Apparent differences in reporting rates according to type of stalking and harassment were found to not be statistically significant, suggesting the means by which the behaviour is carried out does not determine reporting.

Experimental police recorded crime data from England and Wales would suggest that most instances of recorded stalking and harassment relate to more direct and traditional forms of such behaviour. Data for the year ending September 2017[92] shows that 14.6% of such offences were noted as being 'cyber-related'[93]. As yet, there are no equivalent figures for cyber-related recorded crime in Scotland.

Moving away from stalking and harassment, the SCJS captures data on whether respondents have encountered people threatening to damage their property or be violent towards them which made them feel frightened. In 2014/15, 4% of Scottish adults reported experiencing threats (of damage to property or violence) - a figure which has been consistent in each survey sweep since 2008/09[94]. Interestingly none of those reporting experiences of threats said the incidents occurred online. That said, it is considered likely that this is a function of the way threats are described in the survey rather than a true reflection of experiences amongst the population.

Cyber-bullying

In addition to the threatening and abuse behaviour which adults may face online, there are also concerns that the growth in children's use of the internet (across a range of devices) increases the risks of encountering cyber-bullying[95]. It is important to note that whilst harmful and distressing for the individuals involved, it is likely that a high proportion of bullying behaviour will not necessarily amount to a crime.

There is limited available evidence on the extent and prevalence of cyber-bullying, however an EU survey of children does provide some insight here, although findings are caveated[96]. Whilst bullying is defined in quite a general and wide-ranging sense (ranging from 'teasing' to violent actions), the 2013 survey found that 21% of children aged 9-16 in the UK had been bullied in the previous year, with

[92] Crime in England and Wales, Year ending September 2017, Experimental tables, Police Recorded Crime

[93] Cyber-related incidents are defined as cases where the internet or any type of online activity was related to any aspect of the offence.

[94] Scottish Crime and Justice Survey 2014/15

[95] Cyber-bullying is described by ChildLine as: using the internet, email, online games or any digital technology to threaten, tease, upset or humiliate someone else. https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/online-bullying/

[96] Random stratified sample of 516 children who use the internet in the UK. Given the relatively small sample size, the lack of readily available information on the survey methodology, in addition to the age of the data (especially prominent given the growth and advancements in technology), findings should be treated with caution.

12% experiencing cyber-bullying (of some form) and 9% being bullied face-to-face[97].

Considering more timely data in this area, the NSPCC reported that the number of ChildLine[98] counselling sessions carried out in the UK where cyber-bullying was mentioned has almost doubled in recent years, from around 2,250 sessions in 2010/11 to approx. 4,500 sessions in 2015/16[99]. Looking at the two most recent entries (2014/15 and 2015/16), shows there has been a 13% increase. Whilst clearly this data is limited by the fact it will only capture those in contact with the service, and may relate to increased awareness and willingness to report, it does suggest an increasing prominence of online bullying.

Future evidence on cyber-bullying

The CSEW has recently collected data through its module surveying 10 to 15 year olds on bullying including cyber-bullying, and once available this evidence should offer much greater and more robust insight into experiences in England and Wales. Likewise, evidence currently being gathered through the Growing Up in Scotland study should enhance our knowledge in this area and offer a greater understanding of the true extent of cyber-related bullying.

[97] Livingstone, S., et al (2014) Net Children Go Mobile: The UK Report

[98] Twenty-four hour confidential advice and support service for all aged under 19.

[99] How safe are our children?, 2016, NSPCC

3. Cyber-crime as it impacts on businesses

This review now turns to consider the evidence relating to cyber-crime as it impacts on businesses. Following some contextual information, the evidence is presented and discussed in relation to fraud and computer misuse.

Main sources of evidence

The main evidence sources consulted are detailed below, including methodological details and known limitations. Such points should be borne in mind when considering the evidence from these sources.

Source	Details	Limitations
UK Cyber Security Breaches Survey	• Random probability telephone survey of 1,523 UK businesses (i.e. all businesses within scope, had equal chance of being selected to participate). • Includes a 10% Scottish sample. • Fieldwork carried out 24 Oct 2016-11 Jan 2017 • Survey interviews with senior members of staff who have the most knowledge or responsibility for cyber security. • Data weighted to be representative of UK business population by size and included sectors. • Some analysis split by sector and business size: micro 2-9 employees, small 10-49, medium 50-249 and large 250 plus. • Businesses with no IT capacity or other online business presence were excluded from the survey. Although no figures on this are provided, it is noted that this applied to only a small minority of the original sample. • Second survey in this series, with the first covering 2016.	• Excludes sole trader, public sector and forestry, fishing, mining and quarrying sectors. • Estimates of spending and costs associated with cyber security derived from self-reported figures. • Only includes breaches identified by businesses. • Unclear whether 10% Scottish sample is rep. of Scotland. • No regional analysis given. • Not all breaches would necessarily be recorded as crimes under the Home Office Counting Rules. • Some cyber breaches may be dealt with directly by an outsourced provider, in such instances respondents answering to the best for their knowledge.
Commercial Victimisation Survey (CVS) 2016	• Random probability sample of premises. • Telephone survey of 2,962 premises carried out Aug-Nov 2016. • Examines the extent of crimes against business premises in England and Wales. • With each sweep a selection of sectors included. 2016: retail (1,128 respondents), transportation and storage (904 respondents) and administration and support (930 respondents).	• No Scottish sample. • Including different sectors restricts time series data. • Not all incidents would necessarily be recorded as crimes under the Home Office Counting Rules. • Premises based so will not capture incidents occurring at another level e.g. head office.

	• Half of respondents who use computers at their premises are asked about their experience of online crime. This includes: o Hacking o Theft of money o Theft of information o Phishing o Website vandalism o Viruses o Other online crimes • Data is weighted for the sectors surveyed.	• Some crime types, including cyber, tend to affect a business as a whole, rather than affecting individual branches or premises. Thus the CVS is likely to underestimate the scale and prevalence of these crimes. • Crime counts are affected by the size of different industry sectors. • Only includes incidents identified by businesses.
British Retail Consortium (BRC) Retail Crime Survey	• 2016 survey sample covered 37% of the retail sector in the UK by turnover (i.e. retailers survey accounted for 37% of sector turnover). • Sample covered 35% of staff, equivalent to 1.1 million employees. • Appears to be head office based but not 100% clear. .	• Very limited details available on methodology. Not clear how businesses sampled, representativeness, how survey carried out etc. • Membership organisation • UK data only. • Only for retail sector.
Financial Fraud Action: Fraud, the facts 2017	• Reports on data from FFA UK members. • Provides data on card fraud, cheque fraud and remote banking. • All fraud loss figures are reported as gross. These represent the value of fraud including any funds subsequently recovered by a bank.	• Membership organisation • UK data only. • Not clear how data received from organisations is QA, certified etc. • Membership changes could impact on figures and therefore time series analysis not possible.
Cifas Fraudscape 2017	• Reports on data from Cifas National Fraud Database members. • 277 members from across UK public and private sectors.	• Membership organisation. • Not clear how data received from organisations is QA, certified etc. • Membership changes could impact on figures and therefore time series analysis not possible.
Cifas National Fraud Statistics	• Reports on data from members across multiple databases. • Over 400 members in 2016.	• Same as above.
KPMG Small Business and Reputation: The Cyber Risk	• Online survey of 1,000 small businesses. Fieldwork carried out December 2015. • Respondents from 10 UK regions including Scotland. • Small businesses = up to 25 employees, includes sole traders.	• Not apparent how businesses selected. • Findings only apply to those surveyed i.e. not representative. • Small sample size, only 18

	• Businesses from manufacturing, financial services, life sciences, retail and design/creative. • Senior decision makers interviewed in businesses.	businesses in Scotland.
Cyber Security Tracker 2017- Ipsos Public Affairs	• UK panel survey which includes 1,160 SMEs. • Fieldwork carried out 7 Feb-6 Mar 2017.	• For marketing purposes primarily. • Representativeness of sample unclear. • Subject to sampling error. • Data mostly for UK but some Scottish breakdowns provided. • Not apparent what constitutes a SME.
Scottish Business Resilience Centre (SBRC)/Karen Renaud: Survey of small and medium enterprises (SME) 2015/16	• 74 Scottish businesses took part in postal survey and 36 participate in face-to-face or telephone interviews.	• Not apparent how businesses selected, subject to sampling error. • Small sample size. • Not apparent what constitutes a SME.

Context

Internet use

As with the section on individuals, it is important to consider internet and cyber technology usage amongst businesses, in addition to their priorities and use of cyber security measures as a means of providing context to the subsequent findings.

In the absence of Scotland specific data, the 2017 Cyber Breaches Survey provides the most comprehensive and timely UK contextual data. That said, some business sectors (public sector organisations, forestry, fishing, mining and quarrying) and businesses with no IT capacity or other online business presence were excluded from survey. Therefore it is likely that the below figures are higher than we would expect for all businesses across the UK. Yet, the survey does note that only a small minority of the businesses sampled were excluded due to having no IT capacity. References herein to findings from this survey are only representative of included sectors.

At a UK level, the 2017 Cyber Security Breaches Survey reported:

- Almost all (99%) of the UK businesses covered[100] use online services of some form. A large majority have a website (83%), online bank account (73%), electronically hold personal information about customers (61%) and over half (59%) have a social media page. The latter increased by 9 percentage points on the 2016 survey.
- Over half (58%) of UK businesses consider online services a core part of their offering.
- For 74% of UK businesses, cyber security is considered a high priority for senior management and 76% believe core staff take cyber security seriously. Fewer businesses now say it is a very low priority than in 2016.
- The vast majority of UK businesses have cyber security measures in place including applying software updates (92%), malware protection (90%) and firewalls (89%).
- The majority of UK businesses (67%) spent money on cyber security in 2017. By far the most common (unprompted) reason for investing is to protect customer data (51%), up 15 percentage points on 2016. Of note, businesses in Scotland are more likely to cite prevention of fraud or theft (28%, versus 17% overall) as one of their main reasons for investing.
- As to be expected median spend rose in line with business size, with large firms investing £21,200 over the previous year compared to an overall median of £200. Average spend varies widely by sector.

[100] Businesses with no IT capacity or other online business presence were excluded from the survey, in addition to some business sectors.

Research challenges

Within the subsequent sections the review considers evidence which tries to estimate the financial costs of fraud and computer misuse to businesses. In an attempt to contextualise these figures, it is worth noting some of the challenges around deriving such estimates.

Many organisations collect data on the impact of cyber-crime on businesses, however as there is not consistency in how these data are collected across these organisations, it is not possible to present a robust overview of the impact of cyber-crime on business. Nevertheless, it is clear from the available evidence that cyber-crime is an issue for businesses.

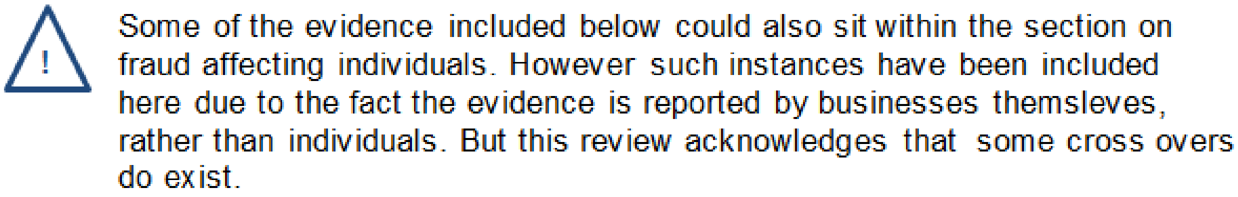
The Costs of Cyber Crime Working Group, established by the Home Office in October 2014, conducted a number of research projects and a review of previous studies to better understand the challenges associated with developing cost estimates. The main issues encountered centred around the inconsistent use of definitions of both costs and cyber-crime, meaning most studies did not measure the same thing, limiting the scope for comparisons.[101] In addition to definitional differences, various studies attempted to measure very different types of cost, as well as different types of cyber-crime. Such challenges are reflected in the evidence included in this review.

[101] Understanding the costs of cyber-crime, Home Office, 2018

Group 3 – Crimes of dishonesty

Summary of findings

- In spite of the challenges highlighted above, it is clear from the available evidence that fraudulent acts are frequently experienced by businesses.
- The 2017 Cyber Breaches Survey found that staff receiving fraudulent emails or being redirected to fraudulent websites was the most common type of cyber breach experienced by UK businesses covered by the survey.
- The 2016 Retail Crime Survey revealed fraud to be the second most commonly experienced crime amongst respondents, accounting for 18% of incidents.
- Available evidence suggests the costs of online fraudulent activities are smaller than costs associated with traditional crimes and amount to a minority of total online transactional values.
- The 2016 Retail Crime Survey estimated that 53% of the total financial cost of fraud against UK retailers is cyber-enabled, representing a total direct cost to the industry of around £100 million. This translates to approx. 15% of the total direct cost of crime against retailers.
- UK evidence from Financial Fraud Action shows in 2016, fraud losses as a proportion spent on UK issued cards stood at 8.3 pence per £100.
- For 2016 Financial Fraud Action estimated value of transactions carried out online using fraudulently obtained cards accounted for 9.5 pence in every £100 spent with UK merchants.



Some of the evidence included below could also sit within the section on fraud affecting individuals. However such instances have been included here due to the fact the evidence is reported by businesses themsleves, rather than individuals. But this review acknowledges that some cross overs do exist.

Fraud as a whole

There are some sources which provide various indications of how fraud can affect businesses. While limitations with the evidence mean we cannot provide definitive conclusions, overall it appears as though fraudulent acts are a common issue and amongst the most frequently experienced crimes by businesses:

- CIFAS[102] recorded 324,683 confirmed cases of fraud via their database of 277 members in 2016[103]. It is not possible to look at time series data, due to the changes in membership.

- CIFAS recorded 16,660 confirmed cases of fraud[104] in Scotland in 2016 via their databases of over 400 UK members. ‘Misuse of facility’ fraud was the most common - 5,827 cases[105]. As with the above, we are not able to look at trends over time due to membership changes.

- Financial Fraud Action UK[106] found that 1.8 million accounts were defrauded via card fraud in 2016 at a value of £618 million[107]. Over 1.4 million of these were remote purchase card fraud[108] at a value of £432 million. The report notes that in the vast majority of such cases card details are obtained through unsolicited emails, phone calls or digital attacks such as malware and data hacks. Whilst the loss of £618 million appears sizeable, for 2016 the FFA estimates that fraud losses as a proportion spent on UK issued cards stood at 8.3 pence per £100. It is not possible to look at year-on-year comparisons due to changes in the organisation’s membership.

- The Retail Crime Survey found fraud[109] to be the second most frequently experienced crime by respondents (behind customer theft), accounting for 18% of incidents in 2016. The 2016 CVS found 7% of incidents carried out against retail premises were acts of fraud[110]. The variations between these two figures is likely attributable to key methodological differences (e.g. coverage, level of measurement etc.) as noted in the source table.

Online fraud

The 2017 Cyber Security Breaches Survey found that 46%[111] of UK businesses identified at least one cyber security breach or attack in the previous 12 months. By far the most common type of cyber breach experienced was ‘staff receiving fraudulent emails or being redirected to fraudulent websites’, identified by 72%

[102] Cifas is a UK wide fraud prevention service representing organisations from the public and private sectors. As part of its remit, Cifas runs a National Fraud Database consisting of data on fraud affecting its members. In 2016 277 member organisations contributed to the database.

[103] Fraudscape 2017, Cifas

[104] Consists of asset conversation; application fraud; false insurance claim; facility takeover; identity fraud; and misuse of facility.

[105] Cifas Fraud National Statistics

[106] FFA represents the UK payments industry and collates data on instances of fraud affecting their members. In July 2017 FFA UK integrated into Finance UK.

[107] Fraud the Facts, 2017

[108] Card details are fraudulently obtained and then used to undertake fraudulent purchases over the internet, phone or by mail order. It is also known as ‘card-not-present’ (CNP) fraud.

[109] Defined by the survey as ‘wrongful or criminal deception intended to result in illegal gain.’

[110] Defined by the survey as ‘where someone cheated the business by diverting funds, goods or services for their own purposes’.

[111] Base 1,523. Only representative of business sectors included.

of businesses suffering a breach.[112] In addition, just over a quarter (27%) of businesses who encountered a breach, experienced 'others impersonating the organisation in emails or online'.

However it is not clear if the survey distinguishes between incidents where staff simply received such emails and those acted on e.g. they responded to emails or disclosed information. This could in part explain why the figure for fraudulent emails is considerably higher than the second most frequently experienced breach.

Analysing data from its UK members, Cifas reports that of the 173,000 cases of identity fraud in 2016, 88% were internet-enabled.[113] Although they provide little explanation as to what internet-enabled amounts to, they do point to the internet as a key contributing factor to the continuing increase of identity fraud amongst its members.

At a premises level, the 2016 CVS reveals experiences of phishing[114] varied according to sector. For premises in administration and support, there were 39 incidents per 1,000 premises in England and Wales, the fourth most common type of online crime[115] in this sector. However for transportation and storage, the figure stood at 2 incidents per 1,000 premises and no rate was recorded for the retail and wholesale sector. This perhaps reflects the high use of computers in the administration and support premises surveyed.[116]

FFA data shows that 14,673 phishing websites[117] were targeted against UK banks and building societies in 2016. The FFA also captures data on case volumes of online banking fraud, which occurs when a fraudster(s) gains access to and transfers funds from an individual's online bank account. Figures show there were 20,088 cases of online banking fraud in 2016.

Costs of online fraud

Based on data from their members the FFA estimates that online card fraud against UK retailers totalled £189.4 million in 2016. Unfortunately no further information on this is provided. Considering the cost of online fraud from a different perspective, the FFA reports on the value of transactions carried out online using fraudulently obtained cards (irrespective of where the card details were sourced). In this respect, the FFA estimates £308.8 million[118] worth of online/e-commerce fraud[119]

[112] Base 781 businesses who experienced a breach.

[113] Fraudscape 2017, Cifas

[114] Defined as having money stolen after being sent fraudulent emails or being redirected to a fake website.

[115] Of those included in the survey: hacking, phishing, theft of money, theft of information, website vandalism, computer virus and other online crimes.

[116] Administration and Support- 92% use computers, Transportation and Storage- 89%, Retail and Wholesale- 84%.

[117] Defined as sending of emails purporting to come from a genuine company such as a bank etc., in an attempt to trick customers of that company into disclosing information at a bogus company website operated by fraudsters.

[118] Included in the earlier card fraud estimates.

took place on cards in 2016, accounting for 50% of all card fraud and 71% of remote purchase fraud. However this equates to only 9.5 pence in every £100 worth of sales for UK merchants being fraudulent. In addition the FFA estimated the value of online banking fraud losses in 2016 as £101.8 million.

The 2016 Retail Crime Survey asked retailers for the first time to estimate the percentage of the total cost of fraud levelled against them that was conducted online ('cyber-enabled fraud'). It was estimated that just over half (53%) of the total cost of fraud was cyber-enabled[120], representing a total direct cost to the industry of around £100 million. Looking at the broader picture, this translates to approximately 15% of the total direct cost of crime against retailers. Although it is important to note that these figures are based on self-reported estimates.

Future evidence – Online fraud

The BRC Retail Crime Survey plans to conduct further work to refine the distinctions between cyber-enabled fraud and cyber-crime, in close collaboration with retailers, to ensure they are able to generate the most accurate picture of the cost of crime occurring online.

Recognising the limitations of CVS (namely that it is measured at a premises level) the Home Office began work with Ipsos MORI to explore the possibility of carrying out a survey of head offices. Following development work, a pilot survey was carried out from February to April 2017 in the Financial, and Wholesale and Retail sectors. The 2017 CVS which is due for release in Spring 2018 will include an update on how the head office survey is to progress.

[119] It is thought that the majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as unsolicited emails or telephone calls or digital attacks such as malware and data hacks.

[120] Involves the use of computers and/or networks.

Group 4- Fire-raising, vandalism etc.

Summary of findings

- 'Computer misuse' is used to capture a number of crimes generally covered by the Computer Misuse Act 1990 and incorporates activities such as unauthorised access (e.g. hacking) and attacks (computer viruses).
- The UK-level 2017 Cyber Breaches Survey estimates that 46% of businesses identified at least one cyber breach or attack between 2016 and 2017. But this data is subject to caveats.
- Incidence of such breaches increases with business size (number of employees) and turnover, in addition to varying by sector.
- The attractiveness of personal customer data to criminals could be increasing the risks for companies holding such information. The 2017 Cyber Breaches Survey found that 51% of UK businesses holding personal customer data experienced a breach, compared to 37% who didn't hold this information.
- Evidence from the UK 2017 Cyber Breaches survey show where businesses experience a breach, incidents of computer viruses, spyware and malware (33%) in addition to Ransomware (17%) are amongst the most common.
- Evidence suggests that staff are viewed as pivotal in the prevention of cyber attacks but are also potentially a weak link in businesses' defences.
- Very few businesses have systems in place to calculate the costs of cyber attacks and there is a lack of consistency in previous research which attempts to estimate costs.
- The majority of businesses identifying a breach do not report them to external bodies and even less report them beyond their cyber security provider. The main reason is that incidents or the impact was not significant enough.

Computer misuse

As mentioned in the corresponding section on individuals, the term 'computer misuse' is used to capture a number of crimes generally covered by the Computer Misuse Act 1990 and incorporates activities such as unauthorised access (e.g. hacking) and attacks (computer viruses). For statistical purposes such acts sit within recorded crime group 4.

Unlike crimes affecting individuals the main evidence source (Cyber Security Breaches Survey) frequently makes reference to 'cyber breaches or attacks' as a whole, rather than the specific activities involved. Such evidence is included here under the heading of computer misuse as the majority of the acts[121] constituting a 'cyber breach or attack' sit within this grouping.

Incidents of computer misuse

The majority of the evidence cited in this chapter comes from the 2017 Cyber Breaches Survey. Whilst it is a valuable UK source, it is important to bear in mind the limitations previously highlighted. Mainly that the survey excludes some sectors (public sector organisations, forestry, fishing, mining and quarrying) in addition to businesses with no IT capacity or other online business presence. Thus references herein to findings from the survey are only representative of the sectors included.

The 2017 Cyber Security Breaches Survey estimates that just under half (46%) of UK businesses identified at least one cyber security breach or attack in the last 12 months[122].

- This ranges from 38% of micro businesses to 68% of larger firms. In addition to rising with business size (number of employees), the incidence of cyber breaches increases with turnover too.

- Breaches are more commonly identified in certain sectors such as information, communications or utilities (62%), administration or real estate (62%) and professional, scientific or technical services (60%)[123].

- UK businesses that hold personal customer data are more likely to have identified breaches (51%), than those that do not (37%).[124]

Of UK businesses identifying cyber security breach or attack in the last 12 months,[125] a third (33%) encountered 'computer viruses, spyware and malware', the second most common type of breach and 17% experienced Ransomware. The analysis makes the link between these sorts of incidents and human behaviour e.g. unwittingly clicking on a malicious link etc., highlighting the importance of staff awareness. What could be classed as more technical breaches e.g. hacking or attempted hacking of businesses' online bank accounts, and Distributed Denial of Service attacks are less common (9% and 8% respectively)[126].

[121] Includes Ransomware; viruses, spyware, malware; website/online services vandalism; hacking/attempted hacking of bank accounts; impersonation of organisation in emails/online; staff receiving fraudulent emails/redirected to fraudulent websites; unauthorised use of computers, networks or servers by staff; unauthorised use or hacking of computers, networks or servers by externals; other.

[122] See sources table and context section for caveats.

[123] Base micro firms-479; large-175; information, communications and utilities-140; admin or real estate-96; professional, scientific or technical-120.

[124] Cyber Security Breaches Survey, 2017

[125] Base 781 who experienced a breach

[126] Cyber Security Breaches Survey 2017

Considering specific sectors, the 2016 CVS found that when excluding 'other online crimes'[127], the incidence rate for computer virus was the highest amongst online crimes for all sectors. This ranged from 155 incidents of computer viruses per 1,000 transportation and storage premises[128] to 78 per 1,000 retail and wholesale premises. Staying with retail, a third of respondents to the 2016 Retail Crime Survey noted their business had seen an increase in Denial of Service attacks over the previous year and a further 30% had experienced an increase in whaling incidents.[129]

Looking solely at cyber breaches amongst small and medium size businesses, the 2017 Cyber Security Tracker revealed that at a UK level 20% of such businesses had experienced a cyber breach in the previous 12 months[130].

Victimisation of computer misuse

Returning to the Cyber Security Breaches Survey, for over a third (37%) of businesses experiencing a breach or attack in the last 12 months, it was a one-time occurrence whilst for 62% it was a more frequent occurrence.[131] Of note, 37% experienced them once a month or more. Large businesses are more likely to be victimised repeatedly, with only 18% experiencing a one-off breach in the last year and 80% subject to multiple breaches[132].

Outcomes and impacts of computer misuse

The Cyber Security Breaches Survey found that 41% of businesses who identified a cyber breach in the previous 12 months noted that it resulted in a material outcome (e.g. loss of assets), translating to 19% of all UK businesses. This could be skewed by the prevalence of fraudulent emails which are less likely to result in an outcome. For those businesses experiencing an outcome[133], the most common was temporary loss of files or network access (23%), followed by corrupted or damaged software/systems (20%).

Looking beyond material outcomes, almost six in ten (57%) firms identified an impact, with 'new measures needed for future attacks' the most frequent (38%), followed by a loss of staff time (34%). The impacts experienced varied by business size with medium and large firms more likely than average to experience any impact (71%).

[127] Any other online crimes which do not fall into the specific online crimes asked about (hacking, online theft of money, online theft of information, website vandalism and viruses).

[128] Base 420 transportation and storage premises, 527 retail premises.

[129] Whaling is a specific kind of malicious hacking which targets people in positions of power and responsibility e.g. company executives, senior management etc.

[130] Base 1,160

[131] Base 781.

[132] Base 120.

[133] Base 339.

Almost nine in ten (89%) of UK small businesses who participated in the 2015 KPMG survey and had experienced a cyber breach[134], felt that the incident impacted on their reputation. Thirty-one per cent noted brand damage, 30% loss of clients and 30% said it impacted on their ability to attract new employees.

In terms of reactions, the Cyber Security Breaches Survey found the most common action taken after a breach is to raise staff awareness via training or communications (28%) rising to 33% amongst firms where breaches resulted in an outcome. Suggesting staff are viewed as pivotal in preventing such breaches and also potentially as a weak link, which resonates with the earlier discussion around the role of human behaviour.

More than half (57%) of businesses noted that it took no time at all to restore business operations after they identified a breach[135]. For a further quarter (23%), this took less than a day, meaning that overall 81% were able to get back to normal in less than a day. Findings from the KPMG small business survey are generally similar. Here it took on average 26 hours for respondents to resolve a breach.

Costs of computer misuse

Attempting to monitor and measure the financial costs of a cyber breach is complex and this may explain why the 2017 Cyber Security Breaches Survey found only 6% of businesses had such systems in place. Consequently, the survey estimated (based on self-reporting) the median cost of breaches identified in the last 12 months, taking account of all impacts. Considering breaches with an outcome[136], the median cost to businesses was £300, rising to £8,230 for large firms. The mean overall cost is markedly higher, highlighting that a minority of businesses experience substantial financial consequences from breaches.

Although only focused on retailers, the BRC 2016 Retail Crime Survey estimated that cyber-crime (defined as crime committed through the use of ICT) represents 5% of the total direct cost of crime to UK retail businesses. This amounts to an estimated direct financial loss to the industry of £36 million per annum. These figures do not include instances of cyber-enabled fraud, as such costs were calculated separately and are discussed in the previous chapter. Thus the vast majority these costs likely stem from incidents under the remit of computer misuse.

Reporting of computer misuse

Analysis from the 2017 Cyber Security Breaches Survey reveals that whilst 92% of businesses flagged breaches to directors and senior management, external reporting is limited. Less than half (43%) of firms[137] reported their most disruptive breach (in the last 12 months) outside their organisation. However this falls to 26% when only considering those who reported a breach to an external body other than

[134] Base-599 businesses who experienced a cyber-breach.

[135] Concerns their most disruptive breach in the last 12 months.

[136] Inclusion of breaches which did not result in an outcome leads to a median of £0.

[137] Base 761.

their cyber security provider. Looking at this in more detail, the most common (unprompted) place to report a breach was a bank, building society or credit card company (28%)[138], followed by the police (19%). Among those who did not report breaches externally[139], over half (58%) attributed this to not considering the breach or its impact to be significant enough, followed by not knowing who to report it to (16%). Suggesting more guidance is needed on why and where businesses should report cyber breaches.

Future evidence on computer misuse

The next release of the Cyber Security Breaches Survey is due in Spring 2018. Whilst the survey is reviewed annually as part of its development, where questions remain unchanged time series data will be available.

The Costs of Cyber-Crime Working Group commissioned a project to devise a costs of cyber-crime framework.[140] Based closely on previous Home Office work, the framework breaks associated costs into three categories:

1. **Costs in anticipation**- normally defensive and preventative measures taken by businesses e.g. training, technology costs etc.
2. **Costs as a consequence**- costs that occur as an immediate result of a crime e.g. business disruption, reputation damage, equipment/infrastructure damage. Businesses tend to have little or no control over these costs.
3. **Costs in a response-** costs that occur as a result of a decision regarding what to do in response to a specific crime. These mostly concern the criminal justice system but incorporates costs incurred through increased IT spending which occurs as a direct result of an incident, change of security provider etc. Businesses are likely to have greater control over these costs.

The costs of cyber-crime framework is intended to enable researchers to identify what the various different component costs of cyber-crime are, and how these combine to form the overall cost of cyber-crime, in addition to costs resulting from specific cyber-crimes e.g. fraud and computer misuse.

It is hoped that the framework will enable greater understanding of research gaps and encourage further, consistent research which can be pulled together to arrive at a more robust and accurate understanding of the cost of cyber-crime and specific crime types. Here, the framework has been discussed in relation to businesses, but it could also be applied to individuals and government entities.

[138] Businesses who reported most disruptive breach to external body other than cyber security provider.

[139] Base identified breach but didn't report externally-432; breach with an outcome but didn't report externally-166.

[140] Understanding the costs of cyber-crime, Home Office, 2018

4. Cyber-crime Offenders

Despite increasing amounts of literature on cyber-criminals, there is very limited data currently available about the perpetrators of cyber-crime in Scotland. Indeed, the very notion that cyber-crimes can be committed remotely creates new opportunities for criminality, meaning (in theory) people can be victimised by criminals in other jurisdictions, and conversely criminals based in Scotland can commit offences against individuals and organisations in other countries.

Whilst there is no apparent Scottish evidence on the extent to which different kinds of individuals and groups account for cyber-crime offences, the National Crime Agency (NCA) assess that the most advanced and serious cyber-crime threat to the UK is the direct or indirect result of activity by a few hundred international criminals typically operating in organised groups[141]. Such groups are highly skilled, sophisticated and competent, and target both individuals and businesses. The NCA also points to a significant number of technically competent cyber criminals being based in the UK.

In spite of the presence of these international groups and technically competent individuals, the NCA asserts that the majority of offenders have relatively low technical abilities, with their attacks often enabled by easy access to bespoke tools, software and expertise online. They believe the availability of such resources may be utilised by young people in particular. For instance, in 2015 analysis of investigations involving the NCA's National Cyber Crime Unit found the average age of suspects to be 17[142].

Returning to evidence gaps, the premise that the majority of cyber-related incidents may go unreported to the police means that rather than offenders being reported and pursued as may be expected for 'traditional' crimes, much of the current knowledge about perpetrators of cyber-crime is derived from the outcomes of pro-active enforcement and investigative work by relevant justice organisations.

Whilst it may be possible to consider what recorded crime records are able to tell us about cyber-related offending, this is not possible on a large-scale given the way the data is currently held and crimes where perpetrators are located out with Scotland will not be captured by police recorded crime data. This is particularly relevant for online crimes given the scope and reach of the internet.

Notwithstanding this limitation the Police Scotland cyber-marker could provide an insight into the perpetrators of some cyber-crimes that come to the attention of the police, where such information is apparent. In due course, the Home Office may release this information for England and Wales police recorded crime, as their cyber flag has been in operation for longer. However any findings would not necessarily be transferable to Scotland.

[141] NCA Cyber-crime Assessment 2016

[142] NCA press release 8 December 2015

5. Conclusions and next steps

Conclusions

This review has drawn attention to the increase in the number of people in Scotland using the internet and the potential for criminals to exploit this growth, under the banner of cyber-crime. There is a lack of clarity and consistency in the terminology used around cyber-crime, and moving forward it may be helpful to start to shift the focus towards cyber-crime being seen as the method or locus of a crime, rather than a distinct type or group.

Whilst this review has found that incidents of cyber-crime tend be concentrated around sexual crimes, fraud and computer misuse, a number of different types of crime can and likely do involve the use of the internet and cyber technologies either as a precursor to a crime or in the committing of a crime itself.

The review has highlighted four key ways in which cyber technology is influencing crime:

1. **Cyber-crime is forming a large proportion of certain crime types.** For example evidence from the CSEW for the year ending Sept. 2017 estimates that over half (56%) of fraud incidents (which is one of the most numerous crimes) were cyber-crimes. This amounts to 1.8 million incidents during this time period.

2. **The internet and cyber technologies are changing the volume of certain crime types.** This is perhaps most evident amongst sexual crimes. Detailed evidence shows that both the number and proportion of police recorded ‘other sexual crimes’ in Scotland which were cyber-enabled increased. Consequently such incidents contributed to the growth in all ‘other sexual crimes’ and sexual crimes as a whole recorded by the police.

3. **The internet and cyber technologies are changing the nature and victimisation of certain crimes.** The police recorded ‘other sexual crimes’ research found that when the specific crimes of ‘communicating indecently’ and ‘cause to view sexual activity or images’ were cyber-enabled the age and relationship profile of victims and offenders changed. When incidents were cyber-enabled, both tended to be younger with median ages of 14 and 18 respectively, and victims and offenders were more likely to know of one another.

4. **Cyber-technologies have given rise to the introduction of an entirely new and high volume category of crime – computer misuse**. Without the internet, these crimes (including computer viruses, hacking etc.) would not be possible. Evidence from the CSEW for the year ending Sept. 2017 shows there were 1.5 million incidents of computer misuse, making it one of the numerous crimes.

However, were are operating in a complex landscape. The review has drawn attention to the challenges faced by authorities to investigate and take action against online risks. These include inconsistent terminology and the spectrum of possible internet involvement in crimes. Such situations also challenge the capability of research and statistics to accurately capture the scale, nature and impact of cyber-crime.

This review has also identified gaps in our knowledge. We still need to know more about cyber-crime in Scotland, such as the prevalence of different types of cyber-crime, the extent of underreporting, the cost and the harm of cyber-crime. Furthermore little evidence is available which allows for the comparison between cyber and non-cyber incidents of the same crime, meaning that it is difficult to ascertain how such crimes differ. This review has also drawn attention to gaps around cyber-crime offenders, in particular the extent to which different kinds of individuals and groups account for cyber-crime offences in Scotland.

Throughout, this review has found evidence that cyber-crime is underreported to the police and other authorities. Figures from the victimisation surveys are consistently higher than in police data, most notably for instances of fraud, computer misuse, abusive/threatening behaviour and stalking and harassment. Suggesting these occurrences are often not being reported to the police. Where apparent, the review has highlighted the possible links between underreporting and the perceived low severity of impacts resulting from many incidents, especially in relation to fraud and computer misuse. Underreporting may be inhibiting the ability of the police to take action and to assign resources accordingly.

Next steps

This review signifies an important first step in collating and assessing existing available evidence on cyber-crime in Scotland. In addition to this review, a number of analytical workstreams are underway across numerous organisations, including:

- **Police Scotland Cyber Capability Review-** a long term piece of work to ensure Police Scotland has a strategic understanding of the cyber-crime threat, and ensure policing is equipped to investigate and respond.
- **Scottish Institute of Policing Research (SIPR)** qualitative research which looks at policing practices from six different countries around the world. This is due to be completed in Spring 2018.
- **HMICS Thematic Inspection of Police Scotland response to Cyber-crime** – scheduled to be carried out in 2018-19.

Furthermore, as this review has alluded to, there are some encouraging signs by way of emerging evidence sources in Scotland. Principal developments include:

- Police Scotland introduced a cyber-marker to their crime recording systems in April 2016. Police Scotland are currently considering how to enhance how crimes with a cyber-element are marked. Identifying a solution requires challenging the definitions and perceptions of “cyber-crime” and acknowledging the limitation of current legacy systems. Therefore improvement will be incremental as definitions and systems develop.

- The SCJS has the potential to capture crimes that aren't reported to or recorded by the police. Whilst the SCJS does currently include a limited number of questions which provide insight on the extent to which the internet and cyber technology was involved in certain incidents, a more comprehensive module on cyber-crime/online behaviour questions will be included in the SCJS questionnaire from 2018/19. A 'cyber flag' question will also be added to the SCJS victim form, allowing us to see the proportion of more traditional crimes which involve the use of the internet. The first findings will be available in late 2019/early 2020 and whilst the data will not be included in the main SCJS incident or prevalence estimates, they represent an important step in developing SCJS evidence in this area. More information is available in the SCJS 2018/19 Questionnaire Review Paper and the full 2018/19 questionnaire will be published in due course.

- It is likely that private companies and businesses including banks, hold useful information on cyber security and incidents where they have been the victim of a crime which occurred online or via cyber technology. The Scottish Government's Justice Analytical Services division is looking to explore this further.

- Although out with Scotland, the CSEW fraud and computer misuse questions are now being asked of the full survey sample (were asked of half sample until October 2017) meaning it may be possible for ONS to provide more detailed analysis and disaggregations, especially relating to incidents of cyber fraud.

- Finally, a number of sources consulted in the review are in their infancy, with little by way of time series data available. As time passes, it will be possible to analyse year-on-year changes and establish any longer term trends, for instance with the CSEW fraud and computer misuse findings.

Going forward it is intended that these developments combined with the above analytical work and existing sources, will contribute to a more complete picture about the influence cyber-technology is having on crime in Scotland.

6. Glossary

Advance fee fraud

Type of fraud where criminals target victims to make advance or upfront payments for goods, services and/or financial gains that do not materialise.

Bank and credit account fraud

Fraudulent access to bank, building society or credit card accounts or fraudulent use of plastic card details e.g. used to make a payment.

Card fraud

Fraudulent activity carried out using bank, credit, debit and charge cards or card details.

Computer misuse

Captures a number of crimes generally covered by the Computer Misuse Act 1990. Activities grouped under this label mainly centre around unauthorised access to and (sometimes subsequent) attacks on computer systems, networks and data.

Consumer and retail fraud

Fraud related to criminals conning an individual into buying something, which is subsequently found to be fraudulent, often through a bogus phone call, email or letter. Examples include online shopping scams and fraudulent computer service calls.

Cyber-dependent crime

Crime committed using computer, networks or other ICT technology. Digital systems are typically the targets of these crimes.

Cyber-enabled crime

‘Traditional’ crimes increased in their scale, reach or speed by the use of computers and the internet.

Cyber security

Computer systems, networks and data are protected from and resilient to cyber threats.

Distributed Denial of Service Attacks (DDoS)

A method of taking an online service (e.g. website) out of action by overloading or ‘flooding’ it with a large volume of traffic from multiple sources trying to access the website at the same time.

Fraud

A crime in which some kind of deception (false representation) is used for personal gain e.g. money, goods/services, information etc. Fraudsters have become increasingly sophisticated and many types of fraud exist.

Hacking

Where criminals break into computers, networks or websites to gain information or to stop an organisation from running as normal.

Identity theft/identity fraud

Type of fraud that involves criminals accessing your personal information (e.g. name, address, DOB, NI number) without consent and using it to impersonate you in order to open bank accounts, get credit cards, loans, and mortgages etc., in your name.

Indicative findings

Are a sign or indication of findings but are not conclusive.

Misuse of facility fraud

The misuse of an account, policy or product e.g. allowing criminal funds to pass through your account or paying in an altered cheque.

Malware, spyware and computer viruses

Malicious software which infects computers, laptops, tablets or mobile phones, stopping them from working properly. In some cases the software also collects information or data saved on devices.

Online banking fraud

When criminals gain access to and transfer funds from an individual’s online bank account.

Other sexual crimes

This is one of four categories used to present statistics on recorded sexual crimes- the others being ‘Rape and attempted rape’, ‘Sexual Assault’ and ‘Crimes associated with prostitution’.

The other sexual crimes category is made up of 41 specific crimes including Communicating indecently, Taking, possessing and distributing indecent photos of children, Sexual exposure, Public indecency and Causing to view sexual images or activity.

Payments industry

Card issuers e.g. banks, credit card companies and card payment acquirers e.g. financial institution that processes credit or debit card payments on behalf of a merchant.

Phishing

Type of fraud where criminals use fake e-mails or websites to obtain personal information and/or to get people to pay money.

Police recorded crime

Crimes reported to, and recorded by, the police.

Random probability sampling

All those within the defined population have equal chance of being selected to participate.

Ransomware

A type of malware that prevents the use of a system or device, e.g. by locking the screen or by locking the users’ files unless a ransom is paid.

Recorded crime/offence groups

Crime groupings used to categorise police recorded crime statistics in Scotland. There are five crime groups and two offences groups.

Remote card fraud

An individual’s card details are fraudulently obtained and then used to undertake fraudulent purchases over the internet, phone or by mail order. It is also known as ‘card-not-present’ (CNP) fraud.

Representative survey sample

Small scale representation of the population from which it is drawn e.g. SCJS sample is adults aged 16 and over living in private households in Scotland.

Statistically significant/statistical significance

Calculated statistically significant differences represent real differences rather than those that may have occurred purely by chance.

Unauthorised access

Gaining access into someone’s computer network without their permission, and then taking control and/or taking information.

Victimisation survey

A survey that asks a sample of people whether or not they experienced any crimes over a fixed period of time. Includes crimes that were not reported to the police. The SCJS and CSEW are examples.

Weighted data

Statistical procedure used to correct for unequal participation in surveys from different groups within the sample. Weighting applied so survey totals match known population totals.

Whaling

Specific kind of malicious attack which targets people in positions of power and responsibility e.g. company executives, senior management etc.

7. Bibliography

Bentley, H., O'Hagan, O., Raff, A., and Bhatti, I. (2016). *How safe are our children?* London: NSPCC.

British Retail Consortium (2017). *Retail Crime Survey 2016.* London: British Retail Consortium.

Cifas (2017). *Fraudscape 2017.* London: Cifas.

Cifas (2018). *Cifas National Fraud Statistics.* London: Cifas.

Financial Fraud Action UK (2017). *Fraud: the Facts 2017.* London: Financial Fraud Action UK.

HM Inspectorate of Constabulary in Scotland (2016). *Crime Audit 2016.* Edinburgh: HMICS

Home Office (2017). *Crime in England and Wales: Year ending June 2017, Experimental Tables, Police Recorded Crime.* Newport: Office for National Statistics.

Home Office (2017). *Crime against businesses: findings from the 2016 Commercial Victimisation Survey.* London: Home Office.

Home Office (2017). *Crime in England and Wales: Year ending June 2017, Bulletin Tables, Police Recorded Crime.* Newport: Office for National Statistics.

Home Office (2017). *Recorded Crime Offence Reference Table.* London: Home Office.

Home Office (2018). *Understanding the costs of cyber-crime: A report of the key findings from the Costs of Cyber-Crime Working Group.* London: Home Office.

Ipsos MORI (2016). *Scottish Public Opinion Monitor June 2016.* Edinburgh: Ipsos Mori.

Ipsos MORI (2017). *Cyber Security Breaches Survey 2017.* London: Department for Culture, Media and Sport.

Ipsos Public Affairs (2017). *Cyber Security Tracker Wave 4.* London: Ipsos MORI.

KPMG (2016). *Small Business Reputation and the Cyber Risk.* London: KPMG.

Livingstone, S., Haddon, L., Vincent, J., Mascheroni, G. and Ólafsson, K. (2014). *Net Children Go Mobile: The UK Report.* London: London School of Economics and Political Science*.*

National Crime Agency. 'Campaign targets UK's youngest cyber criminals', *NCA* (December 8 2015) http://www.nationalcrimeagency.gov.uk/news/765-campaign-targets-uk-s-youngest-cyber-criminals [Accessed February 23 2018]

National Crime Agency (2016). *Cyber-crime Assessment 2016.* London: NCA.

National Records of Scotland (2017). *Mid-2016 Population Estimates in Scotland.* Edinburgh: National Records of Scotland.

NSPCC (2016). *How safe are our children?* London: NSPCC.

Office for National Statistics (2016). *Crime in England and Wales: Year ending September 2016, Experimental Tables*., CSEW. Newport: Office for National Statistics.

Office for National Statistics (2016). *Overview of fraud statistics: Year ending March 2016.* Newport: Office for National Statistics.

Office for National Statistics (2017). *Proportion of adult internet users experiencing negative online incidents, year ending March 2011 to year ending March 2017, CSEW.* Newport: Office for National Statistics.

Office for National Statistics (2016). *Emotional and physical impact of incidents of fraud, by loss (of property or money), Year ending September 2016, CSEW.* Newport: Office for National Statistics.

Office for National Statistics (2017). *Emotional and physical impact of incidents of computer misuse, by offence type, Year ending March 2017, CSEW.* Newport: Office for National Statistics.

Office for National Statistics (2017). *Crime in England and Wales: Year ending March 2017, Experimental Tables*, CSEW. Newport: Office for National Statistics.

Office for National Statistics (2018). *Crime in England and Wales: Year ending September 2017.* Newport: Office for National Statistics.

Office for National Statistics (2018). *Crime in England and Wales: Year ending September 2017, Additional tables on fraud and computer misuse.* Newport: Office for National Statistics.

Office for National Statistics (2018). *Crime in England and Wales: Year ending September 2017, Experimental tables.* Newport: Office for National Statistics.

Peterkin, T. 'Call for Contempt of Court review in internet age', *The Scotsman* (February 22 2015) https://www.scotsman.com/news/call-for-contempt-of-court-review-in-internet-age-1-3697918 [Accessed December 18 2017].

Police Scotland (2017). *Scottish Crime Recording and Counting Standards.* Edinburgh: Scottish Government.

Renaud, K. (2016). *Survey of Small and Medium Enterprises 2015/16.* Stirling: Scottish Business Resilience Centre.

Scottish Government (2016). *Scotland's People Annual Report: Results from the 2016 Scottish Household Survey.* Edinburgh: Scottish Government.

Scottish Government (2016). *Scottish Crime and Justice Survey 2014/15: Drug Use.* Edinburgh: Scottish Government.

Scottish Government (2016). *Scottish Crime and Justice Survey 2014/15: Main Findings.* Edinburgh: Scottish Government.

Scottish Government (2016). *Scottish Crime and Justice Survey 2014/15: Sexual Victimisation and Stalking.* Edinburgh: Scottish Government.

Scottish Government (2016). *Scottish Schools Adolescent Lifestyle and Substance Use Survey (SALSUS): Drugs Summary Report 2015.* Edinburgh: Scottish Government.

Scottish Government (2017). *Recorded Crime in Scotland 2016-17.* Edinburgh: Scottish Government.

Scottish Government (2017). *Recorded Crime in Scotland: Other Sexual Crimes, 2013-14 and 2016-17.* Edinburgh: Scottish Government.

Sheridan, L.P., and Grant, T.D. (2007) 'Is cyberstalking different?', *Psychology, Crime & Law,* vol. 13, 6, pp. 627- 640.

Wall, D.S., (2017). *Crime, Security, and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and its Implications for Regulation and Policin*g. Available at SSRN: https://ssrn.com/abstract=3005872 or http://dx.doi.org/10.2139/ssrn.3005872

UK Government (1990). *Computer Misuse Act 1990*, London: The Stationery Office.

The views expressed in this report are those of the researcher and do not necessarily represent those of the Scottish Government or Scottish Ministers.

This document is also available from our website at www.gov.scot.
ISBN: 978-1-78851-709-6

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

Produced for
the Scottish Government
by APS Group Scotland
PPDAS382446 (03/18)
Published by
the Scottish Government,
March 2018

Social Research series
ISSN 2045-6964
ISBN 978-1-78851-709-6

Web and Print Publication
www.gov.scot/socialresearch

PPDAS382446 (03/18)