Inside out: Characterising cybercrimes committed inside and outside the workplace

Alice Hutchings
Computer Laboratory
University of Cambridge
Cambridge, United Kingdon
alice.hutchings@cl.cam.ac.uk

Ben Collier
Computer Laboratory
University of Cambridge
Cambridge, United Kingdon
ben.collier@cl.cam.ac.uk

***Abstract*—This comparison of cybercrime offenders within and outside the workplace reveals they display very different types of offending behaviour, involving different demographics, initiation pathways, and types of offence. The Cambridge Computer Crime Database (CCCD) is a database of open source information about cybercrime arrests and prosecutions in the United Kingdom. This study analyses data from the CCCD spanning nine years, from 1 January 2010 to 31 December 2018. Insiders are more likely to be older, and commit less-technical offences, primarily data and system breaches. They are less likely to offend with others, the offences are less likely to be international in nature, and they are less likely to receive a custodial sentence. Most alleged offenders are men, but women are more likely to offend within their occupation than outside the workplace. Of those that offend in the workplace, the largest group consists of police officers or police staff. This is likely to reflect differences in the type of organisations that pursue criminal action against insiders. We draw on a strain theory framework to argue that these findings accord with different kinds of strain and differing reactions to strain. The data for crimes outside the workplace support a 'subcultural' pattern of adaptation to strain, with offenders tending to be younger, male and linked to co-offenders. The findings relating to insiders support an opportunity model of crime, with inter-workplace variation in opportunities, working cultures and sources of strain present in different workplaces.**

***Index Terms*—Computer crime, white collar crime, cybercrime, offending in the workplace**

I. Introduction

Cybercrime includes a variety of different types of offences, including gaining unauthorised access to a computer system with or without a further criminal motive, fraud, denial of service attacks, and the development and supply of malware. The cybercrimes included within the scope of this article involve networked computer systems, including the Internet, as well as local networks. This article provides a contemporary, quantitative analytical approach to cybercrime, comparing those that are committed by insiders to those that take place outside the workplace.

A. Cybercrime in the workplace–a form of white collar crime?

Early criminological research into cybercrimes classified them as a form of white collar crime. This is most likely because at the time computers were mainly only available in the workplace [1]. Sutherland, who coined the term 'white collar crime', defined it as a 'crime committed by a person of respectability and high social status in the course of his occupation' [2, p. 7].

Nowadays, the issue as to whether cybercrimes are white collar crimes can be contentious. Sutherland excluded from his definition offenders who did not hold a high social status, including 'wealthy members of the underworld' [2, p. 7]. Since then, the definition of white collar crime has expanded considerably, with Friedrichs [3, p. 211] defining some types of 'technocrime' as a marginal form of white collar crime, and Rosoff, Pontell and Tilman [4, p. 488] referring to cybercrime offences committed by juveniles as 'white collar delinquency'.

On the other hand, Chan [1] asserts that not all cybercrimes can be classified as white collar crimes, particularly unauthorised access. In the 1980s, computers became more widely available to the general public, as did the opportunity to commit cybercrime [5]. This raises the question as to whether cybercrime is a component of white collar crime; or conversely, whether the increasing use of computers in the workplace means that we should rethink this taxonomy, perhaps even classifying white collar crime as a class of cybercrime. The increasing prevalence of digital technology means more offending in the workplace is likely to involve computers [6], [7]. Workplace offenders may not necessarily be of high social status, but the availability of new technologies provides many opportunities for innovation at work, both criminal and legitimate.

B. Cybercrime–offender and offence characteristics

Many cybercrimes (as well as crimes more generally) are committed by young men [8]–[12]. However, these characteristics may actually differ for offences committed in the workplace. For example, an analysis of misuse of computer systems in the Australian public sector found that all suspects were over the age of 34 [13]. Similarly, Clark [14] found that the average age of insiders who had committed cybercrime offences within US companies was 38, and the oldest was 65. This indicates that age of offenders is likely to vary in line with opportunities afforded by the seniority of employees.

Women are also involved in fraud to a greater extent than many other types of crime [15], [16]. Researchers have found

that compared to men, women offenders in the workplace are less likely to hold a senior position [17], [18]. While men are likely to commit the majority of cybercrime offences overall, women cybercrime offenders may be more likely to offend in, rather than outside, the workplace.

The type of cybercrime that is committed may also relate to presented opportunities, as well as the offender's pathway into crime. Hutchings [19] found two different pathways for cybercrime offenders, the 'general' and 'technical' pathways. Those that follow the 'general' pathway are more likely to have experienced particular kinds of strain, such as economic or employment problems, mental health issues, or addictions. They primarily operate alone, but their methods may be inspired by other previous offenders.

Strain theory posits that some kinds of offending can be explained by the inability of individuals to attain widely-held social goals, such as wealth or social status. This experience of strain then leads to them seeking deviant or criminal modes of attaining these goals. Agnew's General Strain Theory extends this into a systematic framework which includes other sources of strain, and factors which may make individuals more or less likely to cope with this strain through criminal offending [20].

Although initially developed to explain offending by economically disadvantaged social groups [21], [22], this framework has more recently been used by Agnew and others to explain white-collar offending [20], [23], [24]. White-collar offending is primarily associated with the blockage of economic goals, especially where there is a perceived injustice on the part of the offender, the presence or threat of economic problems, and work-related stress and dissatisfaction [20]. Some individuals facing these strains attempt to mitigate them, or to achieve their blocked goals, by innovative means. When presented with the opportunity for crime, such as in the workplace, this innovation can include lawbreaking.

Those that follow the technical pathway identified by Hutchings [19] share different characteristics. They tend to offend outside work, primarily operate with others, and their pathway to offending is through associations with others, on and off-line. Through these associations, individuals learn the techniques to commit cybercrime, as well as share the definitions and techniques of neutralisation that justify or excuse their behaviours to themselves and enable offending to occur [19].

The types of strain, and the deviant coping mechanisms offenders may use to mitigate it, are likely to differ for those committing crime in-work and those doing so outside the workplace. For example, those committing crime outside work may be more likely to become involved through the need or desire for social status and monetary gain which they feel blocked from achieving within conventional society. According to subcultural theories of crime, deviant subcultures provide alternative systems of social status within which they are able to achieve these goals. In both cases, status and monetary goals are relative–offenders see themselves as blocked from attaining their goals by legitimate means, and so seek out deviant means of attaining them [22], [25]. Online subcultures, often organised around webforums, often feature in cybercrime–these communities are used for learning and sharing ideologies, recruitment, and trading tools [26]. Thus, this represents a different kind of strain, and a different method of mitigation, from the at-work offenders.

For offending in the workplace, it is likely that offence types and their methods correspond with presented opportunity. To illustrate, the technical pathway would see 'unauthorised access' or 'hacking' carried out with the use of malware or code injection. Alternatively, general methods include 'shoulder surfing', solely employing social engineering techniques, or misusing legitimate access to a computer system [14], [19], [27], [28]. Opportunities for the latter are abundant in the workplace [28]. Insiders may obtain employment at a targeted organisation, be recruited by those attempting to commit offences, abuse their access as the result of becoming discontent in their employment, or become tempted by presented opportunities and the potential perceived gains.

Cybercrimes may also differ according to the extent they cross borders. Leukfeldt et al. [29] analysed police files relating to Dutch criminal investigations and also identified two distinct groups of cybercrime offenders. They call these 'low-tech all rounders' and 'high tech specialists', which broadly correspond to the 'general' and 'technical' offenders identified by Hutchings [19]. They found that that low-tech networks are more likely to incorporate offenders within the same country, and to target local victims, while high-tech networks are more international in nature.

The international nature of the Internet globalises crime, risk and criminal opportunity in complex ways. Offenders in one or more jurisdictions, targeting victims in multiple countries, can commit offences using infrastructure located somewhere entirely different. The requirement for police cooperation across multiple countries can make cross-border cases particularly hard to pursue [30]. Therefore, offences committed locally may be more likely to be investigated and prosecuted.

C. Sentencing outcomes

We also compare sentencing outcomes for cybercrime inside and outside the workplace. This is important because sentencing practices play a key role in establishing how different kinds of criminal behaviour are perceived and constructed. In particular, media reporting on sentencing for white-collar crimes shapes which kinds of workplace fraud or malpractice become labelled as criminal or reported in practice [31]. The use of imprisonment has important consequences for equality and social justice, and can itself cause the further entrenchment of offending behaviour through increasing strain [32].

There is a substantial criminological literature on sentencing, which suggests that disposals tend to vary based on the age, gender, social class of the offender, and the nature of offence [33]–[35]. Use of technical skills, breach of trust, and effects on victims have all been found to be factors in sentencing for cybercrime [36]. Given the characteristics of these offences described above, we would therefore expect to see a disparity in sentencing between cybercrime offending inside and outside the workplace.

D. Reporting insider abuse and workplace type

Insiders can be committing a crime if they access data without authorisation. Insider offences include crimes committed by those who do have authorisation to the computer system, but use that access for unauthorised purposes [37]. This can include access by employees, contractors, consultants, suppliers, and others situated within a workplace [38].

Despite unauthorised access being a crime, it is likely that many employers do not report internal misuse to police. Isenring et al. [39] found that in Switzerland, only 29.3% of the commercial sector and 9.5% of the financial sector report crimes committed by employees to the police. The main reasons for not reporting included reimbursement of the damage by the offender, a lack of evidence, the offence not being serious, and the dismissal of the employee. While the survey did not ask about unauthorised access to computer systems, it did include a category for 'violations of company secrecy', which were least likely to be reported to police. Organisations are most likely to report employee offences when they experience a high level of financial loss.

A reason for not reporting may be concerns about reputation damage. Commercial providers are usually operating in a competitive environment–for example, we can choose with which bank to open an account (although this may be constrained by the availability of bank branches in our area). However, we not only pay for goods and services using financial capital, but also personal information. Our bank knows our income, what we spend it on, where, and when. It can see regular patterns in our expenditure, allowing for the monitoring of routine activities, and perhaps even prediction of future behaviours. Such data allow the bank to detect fraudulent transactions, but may also of interest for a variety of investigatory, marketing, and even criminal, purposes. Companies have an incentive to ensure that their reputation is maintained, to attract and retain customers.

In comparison, individuals have little choice when it comes to governments holding data about them, including school, taxation, health, and council records. There are often particular sensitivities with government-held data. For example, victims who report experiences of crime to the police may be particularly vulnerable. There is also an element of coercion relating to data about those suspected of committing crime. Under the UK's *Investigatory Powers Act* 2016, intelligence agencies and law enforcement can carry out targeted and bulk interception of communications, and bulk collection of communications data. Privacy International allege this data has been accessed improperly, with databases being treated 'like Facebook' to check on birthdays and family members [40].

In this study, data regarding cybercrimes are analysed to test hypothesised relationships with respect to offender characteristics (age and gender), offence characteristics (offence type and nature, international aspects, and involvement of co-offenders), and sentencing outcomes. Workplace type is also examined, to explore which types of organisations report insiders who misuse their computer systems to the police.

II. Hypotheses

We argue that cybercrime offending inside and out of the workplace represent two different categories of criminal behaviour. They tend to enrol different kinds of offenders, demonstrate different pathways to initiation, and involve different types of offences. Drawing from the research literature, we hypothesise that if cybercrime outside the workplace were characterised by subcultural adaptations to strain (such as not achieving social status), offenders would be likely to demonstrate certain characteristics. For example, they would likely be younger, more likely to be men (due to the misogynistic culture of many of these communities [8]), more likely to involve co-offending, and more likely to be international. If, equally, workplace cybercrime fits the model of white-collar strain, one would expect a much higher proportion of women, more opportunity-based crime, and more solo offenders.

We test these relationships through the following hypotheses. The first six test the bivariate relationships between cybercrime offending in and out of the workplace and offender and offence characteristics. The seventh and eighth hypotheses relate to sentencing outcomes, namely the relationship between receiving a custodial sentence, and sentence length, with cybercrime offending in and out of the workplace. The hypothesised direction of these relationships are:

- H_1: Cybercrimes in the workplace involve significantly older alleged offenders than cybercrimes outside the workplace
- H_2: Cybercrimes in the workplace are significantly more likely to involve women alleged offenders than cybercrimes outside the workplace
- H_3: Cybercrimes in the workplace are significantly more likely to be general, rather than technical, than cybercrimes outside the workplace
- H_4: Cybercrimes in the workplace involve different types of offences than cybercrimes outside the workplace
- H_5: Cybercrimes in the workplace are significantly less likely to involve international aspects than cybercrimes outside the workplace
- H_6: Cybercrimes in the workplace are significantly less likely to involve alleged co-offenders than cybercrimes outside the workplace
- H_7: Cybercrimes in the workplace are significantly less likely to receive a custodial sentence than cybercrimes outside the workplace
- H_8: Cybercrimes in the workplace receive a significantly shorter custodial sentence than cybercrimes outside the workplace

For the benefit of those unfamiliar with hypothesis testing, a statistically significant finding does not 'prove' that a relationship exists, but rather provides support for such a relationship. In addition to testing the hypothesis set out above, we use multivariate approaches to confirm the bivariate analyses are not spurious. We also explore the employment sector that cybercrimes in the workplace are from, specifically private organisations, policing agencies, and other public bodies.

III. Method

The data for this research are drawn from the Cambridge Computer Crime Database (CCCD), which records cybercrime events in the UK where someone has been arrested, charged, and/or prosecuted [41]. The database, which is updated weekly, contains 736 entries for 1 January 2010 to 31 December 2018, the period covered for this research. The data in the CCCD are obtained from the public domain. They are harvested from news media, as well as media releases from UK police forces. The database can be accessed from: http://www.cl.cam.ac.uk/~ah793/cccd.html

The CCCD contains cases that are broadly classified as cybercrime offences, including those that fall under the *Computer Misuse Act* 1990. The database also includes cybercrimes that fall under other legislation. This includes fraud, conspiracy, misconduct in a public office, and money laundering offences. Offences that are solely of an interpersonal nature, such as online stalking or harassment, accessing child sexual exploitation material, or online grooming, are not included (although the compromise of computer systems for these purposes, such as gaining access to a victim's email or social media account, are). Also excluded are copyright or online piracy offences, the online sale of illicit, counterfeit or stolen products, or offences where the only computer connection is online planning or communication.

It is difficult to confirm whether the CCCD is exhaustive. This is because offences are usually counted according to the relevant legislation. Many cybercrime cases have not been prosecuted under the *Computer Misuse Act* 1990, but under other legislation such as the *Fraud Act* 2006 or the *Data Protection Act* 1998. Other cases tried under these Acts have little relevance to cybercrime. However, it appears that cybercrime is newsworthy, and many cases are reported in the public domain. Therefore, it is expected that the database provides good coverage of relevant cases.

Of the 736 entries in the CCCD, 34 cases (4.6%) were acquitted or the charges were dropped. These are removed for this analysis, leaving 702 cases. Of these, 522 (74.4%) are considered to be finalised (e.g. sentenced, pleaded or found guilty), while another 180 (25.6%) are unfinalised (e.g. arrested, charged, awaiting trial, or outcome unknown). As we analyse these cases together, the term 'alleged offender' is used to cover cases that are unfinalised, as well as where there has been a conviction, as those in the former category are innocent until proven guilty.

The cases were categorised as to whether or not the offence allegedly took place during or after a course of employment (the dependent variable). This includes offences against a current or former employer, or another individual or business, such as a competitor (excluding setting up a business for the purpose of committing an offence). Sixty-seven cases were excluded, as there was not enough information to enable categorisation. Of the remaining 635 cases, 149 (23.5%) were alleged to have occurred in the workplace.

The independent variables are described as follows:

1) Age: Age at time of arrest or most recent court appearance is known for 602 cases (85.8%), and ranges from 14 to 69 years. The average age is 32.1 years, with a standard deviation of 10.7 years.

2) Gender: Of the 648 cases where gender is known, 530 (81.8%) are men, and 118 (18.2%) are women.

3) General/technical: This captures whether or not the offence requires a particular skill set or knowledge about computer systems. Thirty-six cases are excluded, as there was not enough information to enable categorisation. Of the remaining 666 cases, 358 (53.8%) are categorised as 'general' and 308 (46.2%) are categorised as 'technical'.

4) Offence type: Of the 702 cases, 47 cases were excluded as there was not enough information to enable categorisation. The categories are malware (n=112), data or system breach (n=202), denial of service attacks (n=53), fraud (n=190), and money laundering (n=98). Hardware keyloggers and keyboard, video and mouse (KVM) devices are classified under malware. This category also includes developing, testing of, or providing guides relating to the use of malware.

5) International aspects: This category is coded 'yes' if there was an international co-offender, if they had travelled to the UK to target victims, if they had targeted victims outside of the UK, or had been extradited to the UK. This does not include using cloud services or forums that may be offshore. Of the 645 cases with enough information to enable categorisation, 151 (23.4%) have an international aspect.

6) Co-offending: Of the 702 cases, 471 (67.1%) were alleged to have taken place with at least one co-offender, and 231 (32.9%) involved sole alleged offenders.

7) Custodial sentence: Of the 505 cases where the sentence is known, 305 (60.4%) received a custodial sentence, and 200 (39.6%) received a non-custodial or suspended sentence.

8) Sentence length: The sentence length has been summed for the few repeat offenders. For those that received custodial sentences, the average sentence length is 3.6 years (*SD*=2.6). Sentences range in length from 10 weeks, to 16 years.

As well as analysing the data quantitatively, qualitative narratives have been extracted to illustrate and add context to the research findings.

IV. Results

Hypothesis 1: Relationship between age and offending in the workplace

As is common with offender populations, the distribution is positively skewed, with the majority of cases being younger, as shown in Figure 1. As age is not normally distributed, a Mann-Whitney U test is used to examine the relationship between age and offending in the workplace. As shown in Figure 2, a significant difference is found. Those alleged to have offended in the workplace are generally older (M=37.1, SD=10.3) than those who are alleged to have committed offences outside the workplace (M=30.5, SD=10.2, U=17418.0, $p<.001$), in support of the first hypothesis.

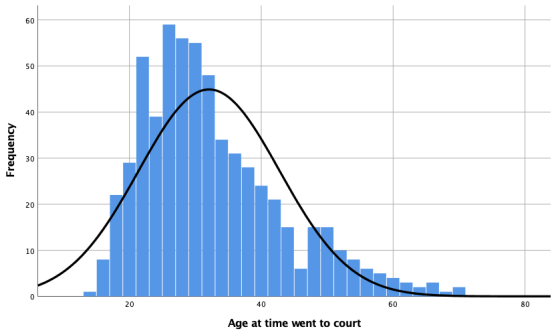

Fig. 1. Age distribution

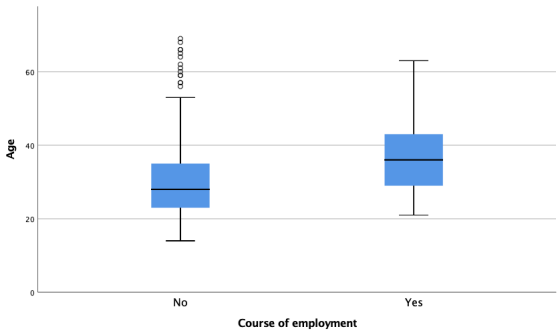

Fig. 2. Age distribution for offending in the course of employment (yes/no)

The ages of those offending in the workplace ranged from 21 to 63. The eldest, a former employee of a community-based counselling charity, pleaded guilty to three offences under section 55 of the *Data Protection Act* 1998. He had sent information relating to vulnerable clients to his personal email address on 11 occasions over a period of eight months. The data included full names, dates of birth, telephone numbers and medical information of 183 people, including three children.

One of the youngest, at 21 years, pleaded guilty to five counts of unauthorised access to computer material, an offence under the *Computer Misuse Act* 1990. She had been a secretary at a county council, where she had accessed extremely sensitive data relating to a victim of child sexual abuse and provided it to her boyfriend, who was one of those accused of the abuse.

Hypothesis 2: Relationship between gender and offending in the workplace

A Chi-Square test of independence is used to examine the relationship between gender and offending in the workplace. As shown in Table I, the relationship between these variables is significant ($\chi^2(1, N=617)=26.05$, $p<.001$). A standardised residual of +/- 2 indicates a cell has a significantly greater, or lesser, than expected frequency [42]. The standardised residuals (highlighted in colour, with blue indicating a greater than expected frequency, and red a lesser than expected frequency) indicate that the women are more likely than expected to offend in the workplace. Therefore, hypothesis 2 is also supported.

TABLE I
CONTINGENCY TABLE FOR OFFENDING IN THE WORKPLACE AND GENDER (EXPECTED FREQUENCIES ARE SHOWN IN PARENTHESIS)

Course of employment	Gender		Total
	Male	Female	
No	404 (382.4) Std. Res 1.1	67 (88.6) Std. Res -2.3	471
Yes	97 (118.6) Std. Res -2.0	49 (27.4) Std. Res 4.1	146
	501	116	617

$\chi^2(1, N=617)=26.046$
$p<.001$

TABLE II
CONTINGENCY TABLE FOR OFFENDING IN THE WORKPLACE AND OFFENCE TYPE (EXPECTED FREQUENCIES ARE SHOWN IN PARENTHESIS)

Course of employment	Offence type		Total
	General	Technical	
No	209 (256.3) Std. Res -3.0	269 (221.7) Std. Res 3.2	478
Yes	124 (76.7) Std. Res 5.4	19 (66.3) Std. Res -5.8	143
	333	288	621

$\chi^2(1, N=621)=80.078$
$p<.001$

One of the largest groups of co-offenders included 21 people. Seven were women, and five offended in the course of their employment. The group targeted corporate banking customers by purporting to be from their bank. Using technology to disguise the number they were calling from–making the phone number appear to be a legitimate bank–they duped customers into revealing personal banking information, allowing them to gain access to their accounts. They then transferred money into 'mule accounts' under their control, and withdrew money from ATMs and bank branches across the country. Of the seven women, five had not offended in the workplace, and instead had committed money laundering offences. The other two were colleagues and sisters, aged just 22 and 24. They worked in the same bank as customer service assistants. They were paid £250 for every bank statement that they provided to the other group members. They both pleaded guilty to conspiracy to commit fraud by abuse of position.

Hypothesis 3: Relationship between general/technical offences and offending in the workplace

A Chi-Square test of independence is performed to examine the relationship between offence type and offending in the workplace. As shown in Table II, and in support of hypothesis 3, the relationship between these variables is significant ($\chi^2(1, N=621)=80.08$, $p<.001$). Offences that take place in the workplace are more likely to be general in nature, such as misuse of legitimate access, and offences that take place outside the workplace are more likely to be technical.

Hypothesis 4: Relationship between offence type and offending in the workplace

A Chi-Square test of independence is used to examine the relationship between offence category and offending in the

TABLE III
CONTINGENCY TABLE FOR OFFENDING IN THE WORKPLACE AND OFFENCE CATEGORY (EXPECTED FREQUENCIES ARE SHOWN IN PARENTHESIS)

Offence category	Course of employment		Total
	No	Yes	
Malware	100 (81.7) Std. Res 2.0	7 (25.3) Std. Res -3.6	107
Data or system breach	71 (149.6) Std. Res -6.4	125 (46.4) Std. Res 11.5	196
Denial of service attack	39 (30.5) Std. Res 1.5	1 (9.5) Std. Res -2.8	40
Fraud	170 (140.4) Std. Res 2.5	14 (43.6) Std. Res -4.5	184
Money laundering	97 (74.8) Std. Res 2.6	1 (23.2) Std. Res -4.6	98
	477	148	625

$\chi^2(4, N=625)=255.809$
$p<.001$

TABLE IV
CONTINGENCY TABLE FOR OFFENDING IN THE WORKPLACE AND INTERNATIONAL ASPECTS (EXPECTED FREQUENCIES IN PARENTHESIS)

Course of employment	International		Total
	No	Yes	
No	309 (342.0) Std. Res -1.8	147 (114.0) Std. Res 3.1	456
Yes	141 (108.0) Std. Res 3.2	3 (36.0) Std. Res -5.5	144
	450	150	600

$\chi^2(1, N=600)=51.474$
$p<.001$

workplace. In support of hypothesis 4, the relationship is significant ($\chi^2(4, N=625)=255.81$, $p<.001$) (see Table III). Cybercrimes in the workplace are significantly more likely to be classified as data or system breaches, and significantly less likely to be classified in any of the other categories. Conversely, cybercrimes outside of the workplace are significantly less likely to be classified as data or system breaches.

A KVM device is a piece of hardware that can be installed on a machine to allow remote access. KVM devices have been used in a number of bank frauds resulting in prosecution in the UK. In one example a bank clerk was caught on CCTV footage accompanying an unidentified man into a customer interview room at the branch. The man inserted the KVM device into a computer, providing access to the bank's systems. Deposits totalling more than £1m were made into genuine customer accounts, and money was then withdrawn, although most was recovered. The 24-year-old bank clerk was found guilty of fraud by abuse of a position of trust.

Hypothesis 5: Relationship between international aspects and offending in the workplace

A Chi-Square test of independence is performed to examine the relationship between offending in the workplace and international aspects. As shown in Table IV, the relationship between these variables is significant ($\chi^2(1, N=600)=51.47$, $p<.001$). Only three of the cybercrimes in the workplace have an international aspect, while cybercrimes outside the workplace are significantly more likely to cross borders.

One of the three cases with international aspects involved the owner of the business, which provided payday loans. He hired people in America to sabotage a consumer rights website after it had carried customers' complaints about his business. He tracked down potential attackers on an online forum, and paid one to try to take the website down, although it did not work. He also paid £2,000 for denial of service attacks against the websites of competitors. He pleaded guilty to five charges of commissioning the attacks.

The other two international cases involved colleagues at a bank who were linked with co-offenders based in Eastern Europe, as well as in the UK. Both employees pleaded guilty. The offences spanned multiple years, during which they had helped launder funds. The money had been stolen using malware sent via email attachment, which allowed remote access to victims' devices and recorded their bank details. The younger of the two had opened 105 of the 199 accounts used to transfer money from a series of UK companies. He also occasionally changed the details of 143 of the 199 accounts. The other had also opened a large number of mule accounts, and had over £16,000 in cash and nine mobile phones hidden in his house. In total, the group laundered more than £16m.

Hypothesis 6: Relationship between co-offending and offending in the workplace

A Chi-Square test of independence is used to examine the relationship between co-offending and offending in the workplace. As shown in Table VII, the relationship between these variables is significant ($\chi^2(1, N=635)=69.29$, $p<.001$). Cybercrimes in the workplace are significantly more likely to involve a single alleged offender, while cybercrimes outside the workplace are more likely to involve multiple people.

Multivariate analyses

We include the variables used for hypotheses 1–3, 5 and 6 (excluding offence type as it has multiple categories) in a forced entry logistic regression analysis to see if the differences disappear when controls for the other variables are used. This allows us to check if any of the relationships are spurious. After excluding 185 cases with missing data, 517 cases were available for analysis: 117 cases where the alleged offender was an insider, and 400 cases where they were allegedly to have offended outside the workplace. Without any independent variables in the model, 77.4% of cases were correctly predicted to have not involved insiders (-2LL=554.6).

The full model was significantly improved with all predictor variables (-2LL=376.6) and was statistically better at predicting if the alleged offender was an insider ($\chi^2(5, N=517)=176.4$, $p<.001$). The full model accounts for between 28.9 and 44.0% of the variance and accurately predicts 85.3% of cases. Of the offences that involved insiders, the model accurately predicts 95.3%.

Table V shows regression coefficients, Wald statistics, odds ratios, and 95% confidence intervals for odds ratios for each of the five predictors. All the variables make a significant contribution to the model.

TABLE V
LOGISTIC REGRESSION MODEL FOR OFFENDING IN THE WORKPLACE

	B	S.E.	Wald	Sig.	Exp(B)	95% C.I. for Exp(B) Lower	Upper
Age	.051	.012	18.542	.000	1.053	1.028	1.078
Gender	.969	.312	9.668	.002	2.635	1.431	4.852
Co-offender	-1.191	.275	18.823	.000	.304	.177	.520
Offence type	-1.824	.313	34.022	.000	.161	.087	.298
International	-2.768	.625	19.620	.000	.063	.018	.214
(Constant)	-1.435	.482	8.879	.003	.238		

TABLE VI
MAIN CRIME CATEGORIES IN AND OUT OF THE WORKPLACE

Inside the workplace	Percentage
Men, data breach, solo	31.7%
Men, data breach, co-offending	22.1%
Women, data breach, solo	18.6%
Women, data breach, co-offending	11.7%
Outside the workplace	**Percentage**
Men, fraud, co-offending	23.9%
Men, malware, co-offending	15.9%
Men, money laundering, co-offending	14.8%
Men, breach, co-offending	7.6%

TABLE VII
CONTINGENCY TABLE FOR OFFENDING IN THE WORKPLACE AND CO-OFFENDING (EXPECTED FREQUENCIES ARE SHOWN IN PARENTHESIS)

Course of employment	Co-offender		Total
	No	Yes	
No	100 (140.8) Std. Res -3.4	386 (345.2) Std. Res 2.2	486
Yes	84 (43.2) Std. Res 6.2	65 (105.8) Std. Res -4.0	149
	184	451	635

$\chi^2(1, N=635)=69.288$
$p<.001$

TABLE VIII
CONTINGENCY TABLE FOR OFFENDING IN THE WORKPLACE AND SENTENCE TYPE (EXPECTED FREQUENCIES ARE SHOWN IN PARENTHESIS)

Course of employment	Sentence type		Total
	Non-custodial/Suspended	Custodial	
No	115 (143.3) Std. Res -2.4	248 (219.7) Std. Res 1.9	363
Yes	82 (53.7) Std. Res 3.9	54 (82.3) Std. Res -3.1	136
	197	302	499

$\chi^2(1, N=499)=32.715$
$p<.001$

The odds ratios indicate that for each additional year of age, the odds the offence took place in the workplace increase by 1.05. If the alleged offender is a woman, the odds the offence was in the workplace increase by 2.64. Having a co-offender, the offence being technical in nature, and having international aspects, each decrease the odds that a cybercrime took place in a workplace by a factor of .30, .16 and .06, respectively.

In Table VI the data is grouped into the four most common categories according to the offender's gender, the type of crime, and whether it was a solo or group offence. This allows us to further explore differences in types of offending. Of offences committed outside the workplace, the four main categories observed were men committing fraud with co-offenders (23.9%), men committing malware offences with co-offenders (15.9%), men laundering money with co-offenders (14.8%), and men committing data breaches with co-offenders (7.6%). We argue, therefore, that cybercrime committed outside the workplace is likely to be characterised by deviant subcultural association as a response to strain.

Inside the workplace, the four main categories were men committing data breaches alone (31.7%) and with co-offenders (22.1%), and women committing data breaches alone (18.6%) and with co-offenders (11.7%). This supports the idea that offenders in the workplace may involve a more opportunity-based form of initiation. This further evidences a clear distinction in patterns of cybercrime offending in-work and outside of the workplace.

Hypothesis 7: Relationship between offending in the workplace and receiving a custodial sentence

A Chi-Square test of independence is used to examine the relationship between offending in the workplace and receiving a custodial sentence. As shown in Table VIII, the relationship between these variables is significant ($\chi^2(1, N=499)=32.72$, $p<.001$). Cybercrimes in the workplace are significantly more likely to receive a non-custodial or suspended sentence.

Hypothesis 8: Relationship between offending in the workplace and length of sentence

As shown in Figure 3, the distribution is positively skewed, with the majority receiving relatively shorter sentences. A Mann-Whitney U test finds that the length of sentence is not significantly different from those that offend outside the workplace ($U=5846.0$, $p=.144$). Therefore, hypothesis 8 is not supported. The distributions are shown in Figure 4.

The longest sentence was 16 years. This was handed down to a 48-year-old police officer who admitted four counts of conspiracy to commit misconduct in a public office, two counts of conspiracy to steal, conspiracy to possess Class A drugs with intent to supply, and conspiracy to possess Class B drugs with intent to supply. He had accessed police computer systems to feed information to a number of criminal associates. An investigation revealed he had been accessing police

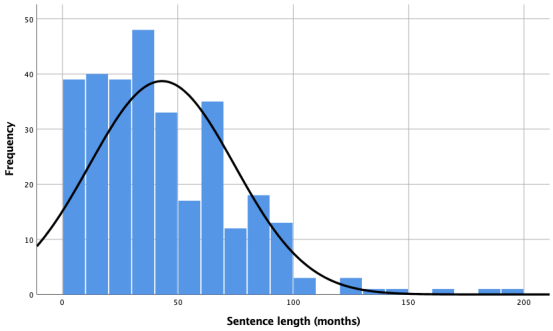

Fig. 3. Sentence length distribution (months)

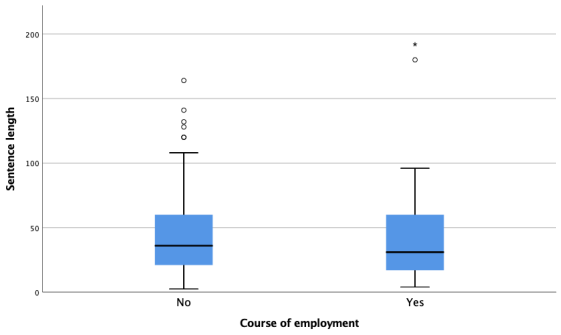

Fig. 4. Sentence length (months) for offending in the course of employment (yes/no)

computer systems and leaking intelligence and information to some of his co-accused from 2011 to 2017.

Type of organisation

The cybercrimes categorised as taking place in the workplace are further analysed to determine the type of organisation involved. Almost half (n=74, 49.7%) were from private organisations, including 19 (12.8%) who worked for banks or financial institutions and 6 (4.0%) who worked for insurance companies. Police employees (officers and staff) accounted for 34.2% (n=51), those who worked for health services, including GPs, hospitals and mental health service providers accounted for 8.7% (n=13), and 7.4% (n=11) were from other public bodies, such as the tax office, schools, or local authorities.

As shown in Table IX, these patterns can be further distinguished by offender and offence characteristics. In private sector organisations, data breaches by men, both solo (29%) and with co-offenders (35%), made up the large majority of crimes, with data breaches by women (6% for solo and co-offenders) and fraud offences by men (6% solo and co-offenders) the next most common offences. In the police, data breaches were similarly prominent, though more likely to include solo male offenders (52%) and women offenders (18% solo, 14% co-offending), with men offending with others making up only 14%. In health and other public sector organisations, data breaches by solo women offenders were much more likely (63%), with data breaches by solo men the next most likely offender type (25%). Finally, for those working in banking or insurance, while data breaches by men or women co-offenders were still the highest category (26% for each), fraud, money-laundering and malware offences were much more likely than for other organisation type. The split in offence categories between these different types of workplace is likely to be due to a combination of a number of factors. These include differences in: opportunities for offending in the workplace; experiences of strain and control factors (including different workplace cultures); and demographic profiles for those employed in certain types of organisations.

Policing agencies have unique opportunities for crime, and may become targets due to the type of data they hold. For example, two police staff (a man and a woman) were found guilty of conspiracy to commit misconduct in a public office. They had attempted to uncover the name of a protected witness who had given evidence at the trial of a 'gangland execution', where two men had been found guilty. The woman was the girlfriend of one of the two jailed, and he was appealing the conviction. He had been sentenced in November 2011 and she started working for the police in January 2012. Two months later, she made her first attempt to unlawfully gather information from the police systems. However, she did not have access to the criminal intelligence system, which contains highly confidential information. She enlisted the help of (and started a relationship with) her male co-offender, who did have access. He made numerous unauthorised attempts to discover the identity of the protected witness and others, and the information gathered was passed on.

In the private sector, financial institutions are a particular target for cybercriminals. A number of examples have already been provided about bank employees committing cybercrimes in order to facilitate other offences. These cases are notable due to the large monetary values and number of co-offenders involved. In another case, a former bank manager was alleged to have printed off confidential customer information, images of customer signatures, and supplied them to unknown others for fraud purposes. While the original charges were dropped, she pleaded guilty to breaching the *Data Protection Act* 1998 by illegally possessing an image of one customer's signature. We note this case follows a similar method to others involving bank insiders, and it is not known to us if they are connected.

V. Conclusion

Within the CCCD, cybercrimes outside the workplace outnumber offences committed during the course of, or shortly after, employment. However, this does not mean that offences are less likely to occur during the course of employment; it may be that employers are less likely to pursue police action for their employees' wrongdoings, and instead resolve these internally. This may also depend on the type of organisation, with police appearing to take a harder stance against illegal access to their databases than private organisations in practice.

The type of workplace offence most likely to be prosecuted is unauthorised access to computer data and systems, a crime type that corresponds with the type of opportunities present in the workplace. As data or system breaches themselves may not create an immediate financial loss to the victimised organisation, a factor that Isenring et al. [39] found was related to organisations being less likely to report to police, it is likely that this is underreported. In addition to financial impact, there may be other reasons for the reluctance to report cybercrimes in particular. These include reputational loss, the time lost to police investigation, and the loss of computers for forensic and evidentiary requirements. Understanding these limitations further may be useful, particularly for identifying ways to encourage businesses to report employee offending by making the process as straightforward as possible. Police may engage in outreach with organisations to demonstrate that they will pursue these types of offences, and could develop streamlined

TABLE IX
MAIN CRIME CATEGORIES IN DIFFERENT WORKPLACES

Crime category	Private sector	Banking and insurance	Police	Health and public sector
Women, breach, co-offending	6.3%	26.0%	14.0%	4.0%
Women, breach, solo	6.3%	0.0%	18.0%	63.0%
Women, fraud, co-offending	0.0%	9.0%	0.0%	0.0%
Women, fraud, solo	2.1%	4.0%	0.0%	0.0%
Women, malware, cooffending	0.0%	4.0%	0.0%	0.0%
Women, money laundering, co-offending	0.0%	0.0%	0.0%	0.0%
Men, breach, co-offending	35.4%	26.0%	14.0%	8.0%
Men, breach, solo	29.2%	0.0%	52.0%	25.0%
Men, DDoS, co-offending	2.1%	0.0%	0.0%	0.0%
Men, DDoS, solo-offending	0.0%	0.0%	0.0%	0.0%
Men, fraud, co-offending	6.3%	9.0%	0.0%	0.0%
Men, fraud, solo-offending	6.3%	9.0%	0.0%	0.0%
Men, malware, co-offending	2.1%	9.0%	0.0%	0.0%
Men, malware, solo-offending	4.2%	0.0%	2.0%	0.0%
Men, money laundering, co-offending	0.0%	4.0%	0.0%	0.0%
Total	100%	100%	100%	100%

procedures so that victimised organisations suffer as little downtime as possible during the course of an investigation. Furthermore, incentives to report, such being able to claim on insurance policies, may be forthcoming as insurance for computer incidents becomes more mainstream.

Overall, seven of the eight hypotheses were supported. Alleged offenders within the workplace differed from those outside the workplace in a number of ways. They were generally significantly older, and while offenders were more likely to be men, women offended in the workplace significantly more than outside the workplace. Offences inside the workplace were less likely to require technical expertise, instead relying on the presented opportunities, and were most likely to involve data or system breaches. In line with Leukfeldt et al.'s [29] findings, they were more likely to be local, with the offences, victims and offenders all being within the UK. As the Internet allows offenders to cross borders with ease, this may indicate that cybercrimes without an international component are more likely to be investigated and prosecuted. They are also significantly less likely to involve co-offending.

When it comes to sentencing, offenders within the workplace are less likely to receive a custodial sentence. However, the hypothesis that those within the workplace who do receive a custodial sentence receive a shorter sentence was not supported, as there was no significant difference in sentence length. This may be due to involvement in other crimes, such as the police officer who was passing information to criminal associates and involved in supplying drugs.

As private organisations make up a smaller proportion of the crimes recorded by the CCCD than might be expected, this indicates that they may be less likely to be victimised, less likely to detect or report these matters to the police, or that they may resolve them internally rather than through public prosecution. Equally, police agencies may be more likely to detect and prosecute misuse of their systems due to the well-established, legally mandated frameworks for accountability, redress and dealing with internal misconduct which they have developed as a public service over the past several decades. As the public generally have no choice when it comes to government agencies holding data about them, the increased willingness of police and other public bodies to formally prosecute insider misuse of data is not misguided.

This analysis supports the overarching hypothesis that in-work and out-of-work offending for cybercrime constitute different kinds of offending, with different offenders, pathways and characteristics. The literature on cybercrime offending suggests that association with deviant online subcultures are important for some kinds of cybercrime, providing potential offenders means to attain status and monetary goals from which they feel blocked, to enrol co-offenders and to learn more advanced technical skills and specialise. The research presented here supports this, suggesting that this may be particularly important for cybercrimes committed outside the workplace. Much of the literature on white-collar crime contends that it is an adaptation to a different kind of strain, and our research suggests that this is the case for 'in-work' cybercrime offences, distinguished by the different opportunities for offending and cultures of different organisations [20]. Cultural factors and the interactions between individuals and the expectations, norms and moral economy of the different social environments they inhabit is likely to play an important role in shaping patterns of cybercriminal offending. This implies that the drivers for offenders involved in different kinds of computer-based offending may not be so different to those in the pre-Internet era.

A limitation in the research design is that the database only contains publicly reported cases that have come to the attention of the criminal justice system. This provides an overview of cybercrimes that have been prosecuted, but not offences that have not been reported. For example, the characteristics of some offenders or offence types may mean they are more likely to be investigated or prosecuted. Furthermore, some employers may be more likely to take internal action, without reporting the matter to the police. Furthermore, cases relating

to sensitive security and intelligence material are not made available in the public domain. However, this research does allow for some conclusions to be drawn about what is missing from the data, particularly for the organisation types that appear to be less likely to report internal misuse to police.

Future work will involve consulting with academics internationally to set up similar databases in other countries. Having equivalent data collection mechanisms and capturing similar variables will allow for comparative studies across multiple jurisdictions. Comparative studies can be used to identify how cybercrime differs across countries, and identify potential variables that affect this, such as economic and policy differences. Cybercrime is increasingly an international issue, and this should be reflected in the data.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their time and insightful comments. Furthermore, this work would not have been possible without the valuable assistance of our colleagues at the Cambridge Cybercrime Centre. In particular, feedback and comments were provided by Richard Clayton, Ross Anderson, Daniel Thomas, and Alexander Vetterl.

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) [grant EP/M020320/1].

REFERENCES

[1] C. Chan, *Is Computer Crime a Form of White-Collar Crime or a New Form of Crime?* University of Leicester, 2003.

[2] E. H. Sutherland, *White collar crime: The uncut version*. Yale University Press New Haven, CT, 1949.

[3] D. Friedrichs, *Trusted criminals: White collar crime in contemporary society*. Belmont, CA: Wadsworth Cengage Learning, 2010.

[4] S. M. Rosoff, H. N. Pontell, and R. Tillman, *Profit without honor: White-collar crime and the looting of America*. Upper Saddle River, NJ: Prentice Hall, 2004.

[5] T. J. Holt and A. Bossler, *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Oxon: Routledge, 2016.

[6] R. G. Smith and P. Jorna, *Corrupt misuse of information and communication technologies*. Cheltenham: Edward Elgar Publishing Limited, 2011, pp. 255–281.

[7] M. L. Williams, M. Levi, P. Burnap, and R. Gundur, "Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory," *Deviant Behavior*, pp. 1–13, 2018.

[8] A. Hutchings and Y. T. Chua, *Gendering cybercrime*. Oxford: Taylor & Francis Group, 2017, pp. 167–188.

[9] A. N. Chantler, *Risk: The Profile of the Computer Hacker*. Perth: Curtin University, 1995.

[10] T. Jordan and P. Taylor, "A sociology of hackers," *The Sociological Review*, vol. 46, no. 4, pp. 757–780, 1998.

[11] D. B. Parker, *Fighting computer crime*. New York: John Wiley & Sons, Inc, 1998.

[12] O. Turgeman-Goldschmidt, "Hackers' accounts: Hacking as a social entertainment," *Social Science Computer Review*, vol. 23, no. 1, pp. 8–23, 2005.

[13] A. Hutchings and P. Jorna, *Trends & Issues in Crime & Criminal Justice No. 470: Misuse of information and communications technology within the public sector*. Canberra: Australian Institute of Criminology, 2015.

[14] J. W. Clark, "Threat from within: Case studies of insiders who committed information technology sabotage," in *11th International Conference on Availability, Reliability and Security (ARES)*. IEEE, 2016, pp. 414–422.

[15] H. Hayes and T. Prenzler, *Profiling Fraudsters: A Queensland Case Study in Fraudster Crime*. Brisbane: Griffith University, 2003.

[16] D. Steffensmeier and E. Allan, "Gender and crime: Toward a gendered theory of female offending," *Annual Review of Sociology*, vol. 22, no. 1, pp. 459–487, 1996.

[17] D. J. Steffensmeier, J. Schwartz, and M. Roche, "Gender and twenty-first-century corporate crime: Female involvement and the gender gap in Enron-era corporate frauds," *American Sociological Review*, vol. 78, no. 3, pp. 448–476, 2013.

[18] J. Goldstraw-White, *White-collar crime: Accounts of offending behaviour*. Basingstoke: Palgrave Macmillan, 2012.

[19] A. Hutchings, *Cybercrime trajectories: An integrated theory of initiation, maintenance, and desistance*. Durham: Caroline Academic Press, 2016, pp. 117–140.

[20] R. Agnew, N. Piquero, and F. Cullen, *General Strain Theory and White-Collar Crime*. Springer, New York, 2009.

[21] R. Merton, "Social structure and anomie," *American Sociological Review*, vol. 3, pp. 672–82, 1938.

[22] A. K. Cohen, *Delinquent Boys*. New York: Free Press, 1995.

[23] N. Langton and N. L. Piguero, "Can general strain theory explain white-collar crime? a preliminary investigation of the relationship between strain and select white-collar offenses," *Journal of Criminal Justice*, vol. 35, pp. 1–15, 2007.

[24] A. Schoepfer and N. L. Piquero, "Exploring white-collar crime and the american dream: A partial test of institutional anomie theory," *Journal of Criminal Justice*, vol. 34, pp. 227–235, 2006.

[25] P. Cohen, *Subcultural conflict and working-class community*.

[26] S. Pastrana, D. R. Thomas, A. Hutchings, and R. Clayton, "CrimeBB: enabling cybercrime research on underground forums at scale," in *Proceedings of the 2018 Conference on World Wide Web*, 2018, pp. 1845–1854.

[27] S. Furnell, "Enemies within: the problem of insider attacks," *Computer Fraud & Security*, vol. 2004, no. 7, pp. 6–11, 2004.

[28] G. Dhillon and S. Moores, "Computer crimes: theorizing about the enemy within," *Computers & Security*, vol. 20, no. 8, pp. 715–723, 2001.

[29] E. R. Leukfeldt, E. R. Kleemans, and W. P. Stol, "A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists," *Crime, Law and Social Change*, vol. 67, no. 1, pp. 21–37, 2017.

[30] R. Broadhurst, "Developments in the global law enforcement of cybercrime," *Policing: An International Journal of Police Strategies & Management*, vol. 29, no. 3, pp. 408–433, 2006.

[31] M. Levi, "The media construction of financial white-collar crimes," *British Journal of Criminology*, vol. 46, pp. 1037–1057, 2006.

[32] S. J. Listwan, C. J. Sullivan, R. Agnew, F. T. Cullen, and M. Colvin, "The pains of imprisonment revisited: The impact of strain on inmate recidivism," *Justice Quarterly*, vol. 30, pp. 144–168, 2013.

[33] J. K. Doerner and S. Demuth, "The independent and joint effects of race/ethnicity, gender, and age on sentencing outcomes in us federal courts," *Justice Quarterly*, vol. 27, pp. 1–27, 2010.

[34] D. Steffensmeier, J. Ulmer, and J. Kramer, "The interaction of race, gender, and age in criminal sentencing: The punishment cost of being young, black, and male," *Criminology*, vol. 36, pp. 763–798, 1998.

[35] K. Daly, "Rethinking judicial paternalism: Gender, work-family relations, and sentencing," *Gender & Society*, vol. 3, pp. 9–36, 1989.

[36] R. G. Smith, P. Grabosky, and G. Urbas, *Cyber Criminals on Trial*. Cambridge University Press, 2004.

[37] Z. Hamin, "Insider cyber-threats: Problems and perspectives," *International Review of Law, Computers & Technology*, vol. 14, no. 1, pp. 105–113, 2000.

[38] J. R. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in *2014 IEEE Security and Privacy Workshops*. IEEE, 2014, pp. 214–228.

[39] G. L. Isenring, G. Mugellini, and M. Killias, "The willingness to report employee offences to the police in the business sector," *European Journal of Criminology*, vol. 13, no. 3, pp. 372–392, 2016.

[40] Privacy International, "Press Release: New court judgment finds UK surveillance agencies collected everyones communications data unlawfully and in secret, for over a decade," 2016. [Online]. Available: https://medium.com/privacy-international/press-release-new-court-judgment-finds-uk-surveillance-agencies-collected-everyones-

[41] A. Hutchings, "Cambridge Computer Crime Database," 2019. [Online]. Available: http://www.cl.cam.ac.uk/~ah793/cccd.html

[42] D. Sharpe, "Your Chi-Square test is statistically significant: Now what?" *Practical Assessment, Research & Evaluation*, vol. 20, 2015.