Measuring the Changing Cost of Cybercrime

Anderson, Ross; Barton, Chris; Böhme, Rainer ; Clayton, Richard; Hernandez Ganan, Carlos; Grasso, Tom; Levi, Michael; Moore, Tyler; Vasek, Marie

Publication date
2019

Document Version
Final published version

Published in
The 2019 Workshop on the Economics of Information Security (WEIS 2019)

Measuring the Changing Cost of Cybercrime

Ross Anderson [1] Chris Barton [2] Rainer Böhme [3] Richard Clayton [4]
Carlos Gañán [5] Tom Grasso [6] Michael Levi [7] Tyler Moore [8] Marie Vasek [9]

Abstract

In 2012 we presented the first systematic study of the costs of cybercrime. In this paper, we report what has changed in the seven years since. The period has seen major platform evolution, with the mobile phone replacing the PC and laptop as the consumer terminal of choice, with Android replacing Windows, and with many services moving to the cloud. The use of social networks has become extremely widespread. The executive summary is that about half of all property crime, by volume and by value, is now online. We hypothesised in 2012 that this might be so; it is now established by multiple victimisation studies. Many cybercrime patterns appear to be fairly stable, but there are some interesting changes. Payment fraud, for example, has more than doubled in value but has fallen slightly as a proportion of payment value; the payment system has simply become bigger, and slightly more efficient. Several new cybercrimes are significant enough to mention, including business email compromise and crimes involving cryptocurrencies. The move to the cloud means that system misconfiguration may now be responsible for as many breaches as phishing. Some companies have suffered large losses as a side-effect of denial-of-service worms released by state actors, such as NotPetya; we have to take a view on whether they count as cybercrime. The infrastructure supporting cybercrime, such as botnets, continues to evolve, and specific crimes such as premium-rate phone scams have evolved some interesting variants. The overall picture is the same as in 2012: traditional offences that are now technically 'computer crimes' such as tax and welfare fraud cost the typical citizen in the low hundreds of Euros/dollars a year; payment frauds and similar offences, where the modus operandi has been completely changed by computers, cost in the tens; while the new computer crimes cost in the tens of cents. Defending against the platforms used to support the latter two types of crime cost citizens in the tens of dollars. Our conclusions remain broadly the same as in 2012: it would be economically rational to spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more on response. We are particularly bad at prosecuting criminals who operate infrastructure that other wrongdoers exploit. Given the growing realisation among policymakers that crime hasn't been falling over the past decade, merely moving online, we might reasonably hope for better funded and coordinated law-enforcement action.

[1]Computer Laboratory, University of Cambridge, Cambridge, UK. ross.anderson@cl.cam.ac.uk
[2]chris@vnworks.net
[3]Department of Computer Science, Universität Innsbruck, Innsbruck, Austria. rainer.boehme@uibk.ac.at
[4]Computer Laboratory, University of Cambridge, Cambridge, UK. richard.clayton@cl.cam.ac.uk
[5]Faculty of Technology, Policy and Management, Delft University of Technology, Delft, Netherlands. C.HernandezGanan@tudelft.nl
[6]Qintel, Pittsburg, PA, USA. tom@qintel.com
[7]School of Social Sciences, Cardiff University, Cardiff, UK. levi@cf.ac.uk
[8]Tandy School of Computer Science, The University of Tulsa, Tulsa OK, USA. tyler-moore@utulsa.edu
[9]Department of Computer Science, University of New Mexico, Albuquerque NM, USA vasek@cs.unm.edu

1 Introduction

As everything has gone online – including crime – governments struggle to keep up, and want to know how much should be spent on cybersecurity. Policymakers want accurate statistics of online/electronic crime and abuse. However, many of the existing surveys are carried out by organisations (such as security vendors or police agencies) with a particular view of the world and often a specific agenda. We therefore wrote a survey paper on 'Measuring the Cost of Cybercrime' which set out what was known, and what was not, at the beginning of 2012 [4]. It built on a report written by four of us in 2008 for the European Network and Information Security Agency, 'Security Economics and the Single Market' [5]. Both reports analysed the statistics available at the time, their shortcomings, and the implications for policy.

Seven years on, the world has changed. Most people now have smartphones, which have displaced PCs and laptops as the main way to get online. Electronic banking and commerce have grown in both volume and value. Many people live much of their lives on social networks. New apps, such as ride hailing, and new technologies, such as cryptocurrencies, create new targets, while old targets such as medical records have migrated to cloud services. So larger quantities of personal information are kept online, and are open to a variety of attacks. Ever larger security breaches are reported. The Snowden and other revelations have taught us about what intelligence agencies get up to.

So what has changed in the world of cybercrime? This paper sets out to answer that question.

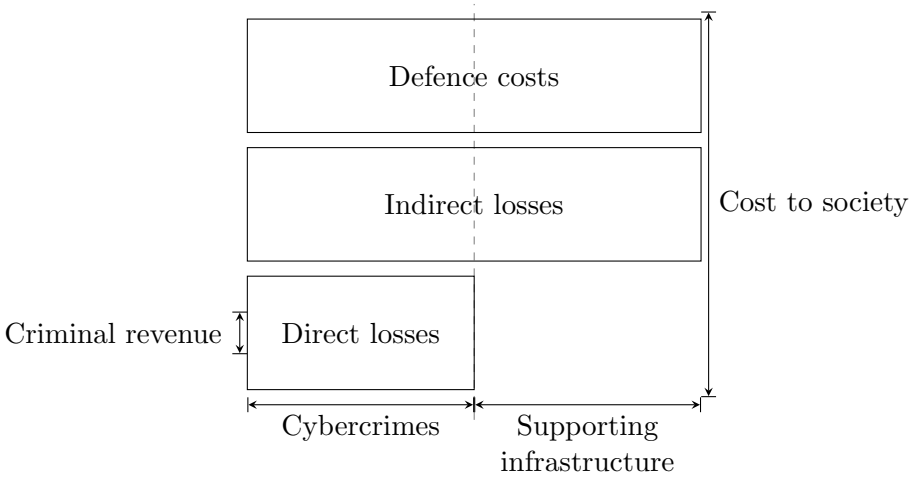
We begin by describing our framework for analysing the costs of cybercrime in Section 2, differentiating cybercrimes from physical ones and decomposing cost categories; this is the same framework we used in 2012. Next, in Section 3 we work through all relevant types of cybercrime, the cybercriminals' profit centres, and present such data as we have about how much they earn as well as the identifiable indirect costs. However, many of these activities rely on criminal infrastructure, based on botnets, which impose costs on the owners of subverted machines and also on society more broadly in the form of indirect and defence costs. These costs cannot for the most part be attributed to individual crimes and are discussed separately in Section 4. Section 5 then discusses what we now know from victimisation studies, which provide us with valuable new ground truth about how many crimes their really are, while Section 6 presents our conclusions.

2 Our Framework for Analysing the Costs of Cybercrime

It has always been hard to define and measure white-collar crimes. Periodic scandals (McKesson & Robbins in 1938, IOS and Equity Funding in 1973, Enron in 2001, the banking crisis in 2008) have raised questions about which business practices should be outlawed, leading to changes in both legal and accounting definitions, regulations and practices. These shifts are associated with changes in social attitudes and political discourse; for a discussion see [53, 54].

Measurement is not straightforward, as cybercrimes frequently cross jurisdictions, and the available statistics are fragmentary. As in our 2012 paper, we will proceed on a best-efforts basis. In some cases (as in payment card fraud) we have figures for some jurisdictions only, while on other cases (such as botnet operations and some cryptocurrency-enabled scams) we have only global figures, so we will simply scale the available figures up or down as appropriate. Where there is reason to believe that national figures are out of line with other countries, we will say so and make an appropriate allowance.

Figure 1: Framework for analysing the costs of cybercrime



As in our 2012 paper, we follow the European Commission's 2007 Communication "Towards a general policy on the fight against cyber crime" [26], which proposed a threefold definition:

1. traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems;
2. the publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to racial hatred);
3. crimes unique to electronic networks, e.g., attacks against information systems, denial of service and hacking.

To have a yardstick with which to measure changes, we break down fraud figures as follows.

We split direct costs from indirect costs, accounting for the costs of security (which often cannot be allocated to specific crime types) and for the social and opportunity costs of reduced trust in online transactions. Where possible we decompose the costs of crime still further, splitting the criminals' revenue from the costs they impose on others (which are often very much larger). Figure 1 shows our framework, and its cost categories are as follows.

Criminal revenue is defined as the gross receipts from crime. It does not include the criminal's 'lawful' business expenses,[1] but we do need to count criminal inputs, so as to get an accurate estimate of the criminal-revenue contribution to GDP. For example, where phishing is advertised by email spam sent by a botnet, we add the criminal revenue of the phisherman (the money withdrawn from victim accounts) and the amount he pays the spammer – possibly split with the 'owner' of the botnet.

Direct loss is the value of losses, damage, or other suffering felt by the victims as a consequence of a cybercrime. Examples include money withdrawn from victim accounts; time and effort to reset account credentials after compromise (for both banks and consumers); and lost attention and bandwidth caused by spam messages.

[1]The UK Proceeds of Crime Act does not allow an offender's costs to be deducted from the amount he is deemed to owe the state

We do not try to measure distress directly; victims are not generally entitled to sue for it and it is hard to measure.[2] Instead we try to estimate the chilling effect that cybercrime – and the fear of cybercrime – have on economic activity. This brings us to:

Indirect loss is the value of the losses and opportunity costs imposed on society by the fact that a certain type of cybercrime is carried out. Indirect costs generally cannot be attributed to individual perpetrators or victims. Examples include loss of trust in online banking, leading to reduced revenues from transaction fees and higher costs for maintaining branch staff; sales foregone by online retailers when their fraud engines cause them to decline shopping baskets; reduced uptake by citizens of electronic services whether from companies or governments; cancelled operations due to online medical services being unavailable; and efforts to clean up machines infected with botnet malware.

Defence costs measure prevention efforts. They include security products such as spam filters and antivirus; security services provided to individuals, such as awareness raising; security services provided to industry, such as website 'take-down' services; fraud detection and recovery efforts; law enforcement; and opportunity costs such as the inconvenience of missing messages falsely classified as spam.

Like indirect losses, defence costs are largely independent of individual perpetrators and victims – and even of individual types of cybercrime.

In our model, the total social cost of cybercrime is the sum of direct losses, indirect losses, and defence costs. All our figures are in nominal terms. We neglect inflation, as a 2012 dollar is worth $1.11 in 2019 dollars, and the 11% difference is way below our error margin; interest rates have also been near-zero for most of this period. Similarly, differences in exchange rates are insignificant. We are not going to obsessively translate all amounts back and forth between pounds, dollars, and Euros; with the accuracy with which we can work here, these currencies might as well be interchangeable.

2.1 Discussion of the framework

We showed in 2012 that criminal revenue is significantly lower than direct losses and much lower than total losses. For example, a botnet that earned about $3m a year by promoting Viagra was costing about a hundred times that much, as it was responsible for about a third of the world's spam in 2011 – and spam cost the industry about $1bn a year [52]. This raised the policy question of who will (or should) pay to stop it. A company may invest in protection to the extent that it reduces its direct costs, while a government might invest in collective defence efforts such as policing to optimise social welfare overall.

Government spent very little fighting cybercrime in 2012,[3] and the situation is largely unchanged.[4] There are both political/behavioural and economic factors in play. The widely different budgets for fighting different crimes can be analysed in terms of psychological salience: 'signal crimes' [42] such as terrorism demand political action. But thanks to spam filtering, spam is no longer salient to most citizens in the way that terrorism is.

[2]This largely excludes crimes of the second category of the EC definition: publication of illegal content over electronic media

[3]The USA spent about $100m at the federal level and the same again at state and local level, while countries like the UK and Germany spent in the low tens of millions – an order of magnitude less. In the private sector, Microsoft and Google spent about $100m each, Facebook maybe $40m and other service firms still less – but the fraud and abuse teams in these firms targeted specific harms and specific parts of the criminal infrastructure.

[4]The DoJ has a cybersecurity budget of $721m for 2019 but the lion's share goes on defensive measures and to the FBI's intelligence functions rather than on fighting cybercrime. The same holds for the UK's £300m a year.

Economic models also provide useful insights. Globalisation means that for much online crime, the perpetrators and victims are in different jurisdictions, reducing both the motivation and the opportunity for police action. Outside the EU, mutual legal assistance was not intended for routine police and criminal justice cooperation but for rare and serious cross-border crimes. Industry incentives remain mixed: the real winners from spam may be firms like Google, Microsoft, and Facebook as people are driven to webmail services with their better spam protection or switch to instant messaging services.

We will return to this complexity later. In the next two sections we collect what is known about the actual costs.

3 What We Know

Few of the existing measures of cybercrime try to unbundle the different types of crime and categories of cost described above. In the following two sections, we summarize what is known and how it has changed since 2012.

3.1 Online card fraud

Bad things on the Internet most commonly affect real citizens when a charge they don't agree with appears on their credit card statement or bank statement, and so payment fraud trends are a bellwether of online property crime overall. The big picture is that payment fraud has about doubled in total value since 2012, but it has fallen slightly as a percentage of turnover. In other words, the world's electronic payment systems have got much bigger, and slightly more efficient. There is a caveat in that we've seen the emergence of new types of financial fraud.

In 2012, we reported UK card fraud of £441m (which were figures from 2010). The 2017 industry figures, reported in 2018, show a total of £731.8m, and claim that a further £1.4bn of attempts were stopped [89]. In more detail, card-not-present fraud about doubled in volume and value, with e-commerce fraud rising while mail order and telephone order fell; e-commerce losses are now 55% of the total. Meanwhile lost/stolen card fraud tripled in volume but only doubled in value; and counterfeiting fell; see Figure 2 overleaf for more detailed breakdown and trends. These are all as one might expect given growing online business, better fraud analytics and the ever wider adoption of chip cards. (There is still an issue with cards being copied by skimmers in the UK and mag-strip clones being used overseas in countries that haven't fully adopted chip card technology.)

Our measure for the fear of crime was based on Eurostat's ICT survey, according to which 14% of UK consumers stated in 2010 that they refrained from buying goods or services online because of security concerns; taking into account that many of these sales happened offline instead, we estimated the cost of sales foregone due to lack of customer confidence at $700m. The current Eurostat figures show that Internet access and online shopping are both up since 2012 though the figures are not directly comparable.

As for caution on the part of merchants, we relied on a survey of online merchants carried out by Cybersource, a VISA company that does credit card processing [49]. Merchants reported lost revenues of 1.8% of turnover, mostly to chargebacks, of which 32% were ascribed to fraud; and rejected 4.3% of orders out of fear of fraud. Overall, we assessed the indirect losses at 1% of the UK's 'digital economy', then £100bn or 7.2% of GDP [45] (of which only half was actual online shopping) giving us indirect losses of $1.6bn. Their 2019 report breaks down figures by region;

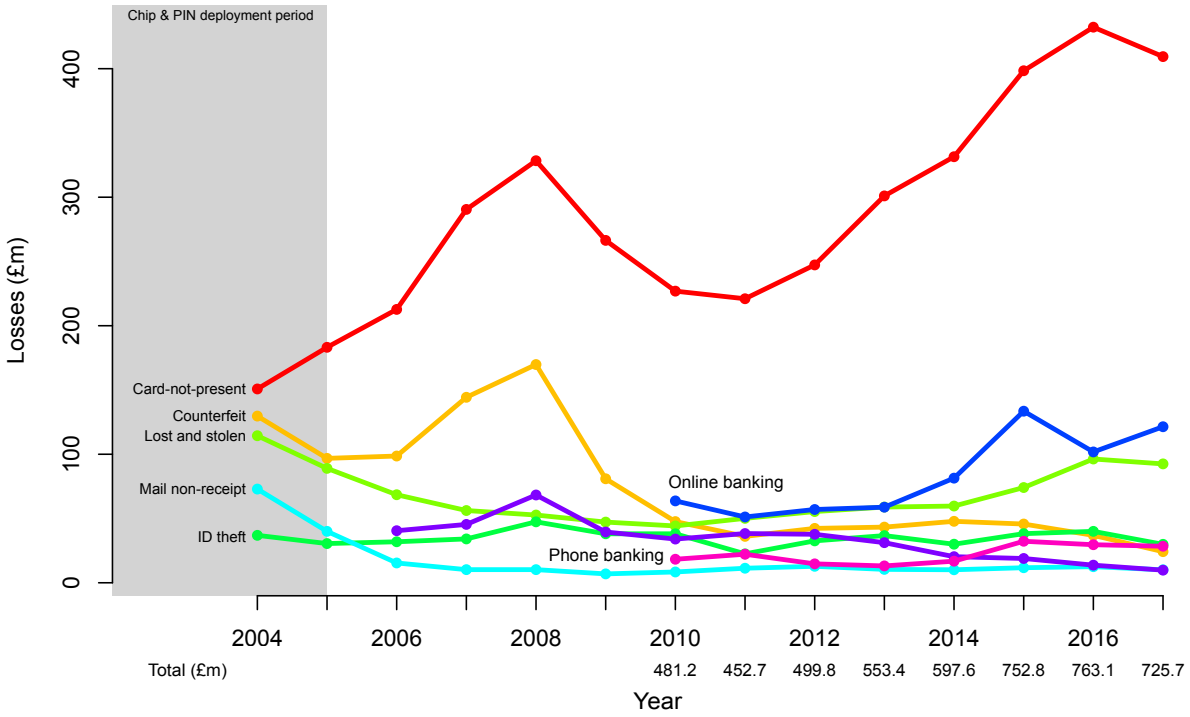


Figure 2: UK card fraud by category during and since the introduction of EMV ('chip and PIN') (Source: UK Payments Administration)

for the USA and Europe, revenue losses are down slightly to 1.5% (of which chargebacks are 0.7%) while rejected orders are down to 3% [22]. These support the same general conclusion: that while payment volumes have about doubled, merchants have also improved their fraud detection technology.

After a bulk card compromise, issuers must decide whether to reissue cards to mitigate fraud and reassure consumers. Graves et al. estimate from public sources that the cost of reissuing cards ranges from $5 to $25, with a point estimate of $10 [33]. Not all cards are reissued following a breach, but the same authors identify (again from public reports) that between 80–95% of cards are reissued. We inspected all reports from the Privacy Rights Clearinghouse [78] that mentioned "card" in the breach description, then manually confirmed whether unencrypted payment card information was exposed.

Because these publicly-sourced data are incomplete, we can estimate a lower bound for the number of compromised cards for 2018 to be 11.2 million. This corresponds to an estimated cost for reissuing cards of $98m. For 2017, 4 million cards were exposed, which would trigger a reissuing cost of $35m. This does not include lost business to card issuers during downtime when the replacement card is shipped. This cost can be substantial if customers switch to an alternative card or payment method in online accounts and never change back after a replacement card is reissued [79, Chapter 6]. As it merely redistributes revenue between services, often in favour of larger players, this effect does not translate directly to welfare losses.

3.2 Online banking fraud

We treated online banking fraud separately from card fraud in 2012, as the modus operandi was different: credentials were typically phished or stolen using malware. The figures were also less reliable, as customers are often blamed for the fraud, even more than is the case with disputed card transactions. The scale can also vary, from bulk phishing using forged bank websites to sophisticated spear-phishing attacks on businesses.

According to the official UK figures, online bank fraud more than doubled, from £51.1m in 2011 to £121.4m in 2017. (In our 2012 paper, we estimated only $24m based on global studies of phishing and malware proceeds; UK banks started collecting data in 2009 but did not combine them into case volumes until 2012.) There's a separate heading for phone banking fraud, up from £22.2m in 2011 to £28.4m in 2017.

The ECB has European card fraud figures, with its fifth oversight report covering developments from 2012–6 [25]. In 2016, fraud against Euro-area cards was €1.8bn, and as a percentage of transactions was slightly down at 0.041%. Of this, card-not-present was the largest slice at €1.32bn and was the only component that was growing; ATM and POS fraud was falling rapidly. Issuer fraud rates were very skewed across countries, with Denmark over 0.07% and the UK and France almost at that level, while the rates for Greece, Hungary, the Czech Republic, Slovakia, Romania, Poland and Latvia were under 0.01% (though in most of these countries they are growing rapidly). The ECB also tells us that fraud rates are strongly correlated with levels of card use. We should therefore be slightly cautious about scaling up UK card fraud rates to Europe as a whole, since the UK has long been the most extensive and mature card-using market in Europe.

The most recent upset has been the rapid growth of authorised push payment (APP) scams, a category not previously reported, which accounted for a further £236m over 43,875 incidents. In an APP scam, a bank account holder is tricked into transferring money to the fraudster, who typically poses as a bank employee and uses some combination of social engineering skills and technical mechanisms. According to UK banks, the difference is that in an APP scam the customer authorised the transaction while in an online banking fraud they did not. The Payment Services Regulator proposes to direct large UK banks to provide a 'confirmation of payee' (CoP) service by March 2020.[5] Thereafter there will be a code of practice urging the banks to accept more liability for APP; it remains to be seen how this will evolve since doubtless the crooks will continue to figure out how bank systems can facilitate misdirection attacks. APP scams target individuals and there is a clear overlap with Email Account Compromise (EAC) which we discuss in Section 3.10 in conjunction with Business Email Compromise (BEC) where fraudsters raid corporate accounts by tricking employees into initiating payments from them.

The latest development in bank fraud is mobile malware. Many banks use SMS for two-factor authentication, but Android apps can listen to any incoming SMS (assuming the user gives consent, which is usually granted without thought). There has been an uptick in frauds based on SMS stealing, but we do not yet have any dependable numbers.

As for the costs of defending against online bank fraud, some are generic – rapid patching, antivirus and so forth – while measures specific to online banking include contractors who take down phishing websites, and vendors of authentication systems. In 2012 we estimated their collective turnover at $500m and added a similar amount for the banks' internal security development costs getting an estimate of $1000m globally for securing online banking against

[5] When you make your first payment to another account, you'll enter the payee name as well as the account number and sort code, whereupon you'll be told whether it matches, almost matches, or doesn't match at all.

specifically cyber threats; we added a further $2,400m for the costs of securing card payment networks (see Section 3.3 below). Both figures may have been an underestimate, but hard figures are as difficult to get now as they were then. A survey of financial institutions suggested that large publicly quoted firms may spend $50–200m on IT security (which might be double that of non-financial companies of comparable size), while large private firms may spend $20m more [23], so presumably a lot of the expenditure represents compliance costs rather than risk reduction. Given that the UK has six large banks and a number of smaller players, financial information security expenditures may be of the order of a billion, and the risk-reduction component somewhat less than half of this. (The banks also supply many merchant terminals but we consider this in the following section.)

As for indirect costs, we worked from Eurostat figures suggesting that security concerns keep 16% of UK residents from doing online banking to estimate a 2010 cost of £450m, or $700m, shared between consumers and banks, but noted that this was highly uncertain. The Eurostat statistics only go up to 2015, but as online participation has increased, loss of sales due to fear of fraud has presumably fallen. It is not even clear that low uptake is a robust measure of fear, given the wide variation between countries and the rapid increase in card use in low-uptake states. The best figures we have for the chilling effect come from the Belgian victimisation study described in Section 5.3: about 6% of respondents said they limited their online banking activities, and 10% their online shopping, as a security measure.

3.3 In-person payment card fraud

In 2012, we noted that the fall in counterfeit UK transactions since the introduction of EMV had been matched by a growth in fraudulent overseas transactions, which amounted to £93.9m ($147m) by 2010. It seemed sensible to account for 'online and electronic' fraud, a category that includes card fraud perpetrated in person. The official UK figures simply give a total for all overseas card fraud, and that has risen to £158.4m in 2017 (down from a peak of £200.2m in 2016), lumping in losses from mag-stripe clones of cards skimmed at UK ATMs and POS terminals along with remote purchase fraud at overseas retailers.

The ECB figures tell a similar story, but with more detail. Almost all counterfeit fraud against European cards is now at terminals outside the EU, while fraud in general is becoming more cross-border within the EU: non-EU transactions are steady at about 22% while within-EU cross-border transactions have grown from 25% to 43% from 2012–6.

We estimated in 2012 that the defence costs of EMV deployment were roughly equal to the $2.4bn total worldwide market for payment terminals, reasoning that although the total cost of deployed systems may be about three times that, most of their cost is about providing functionality rather than security.

The worldwide market now appears to be several times larger, given the US rollout of EMV beginning in 2015, the arrival of contactless NFC payment leading to a surge in fixed terminal replacement, and rapid growth in mobile terminals. Hard figures are difficult to come by, though; most merchants rent terminals from banks and the cost is buried in transaction fees. Some market reports put the worldwide total around $40bn, though this may include equipment such as store checkout lanes. Given that card transaction volumes have doubled, we might go for a conservative figure of $5bn. We suspect that the cost per terminal must be falling because of low-cost offerings from firms like Square and iZettle that cost in the tens of dollars.

3.4 Ransomware and cryptocrime

While ransomware has been around for over a decade, the rise of cryptocurrencies has enabled this particular type of malware to flourish. In the first three quarters of 2012, there was an estimated £1.9m–3.8m lost to ransomware [72]. These payments were made by prepaid money cards such as Paysafecard, Ukash, and Moneypak. After the malware authors adapted to cryptocurrencies, their revenues increased substantially. Research done by Liao et al. on CryptoLocker, a particular Bitcoin-based ransomware program, from a 5 month period 2013 through 2014 showed $300,000-$1,100,000 lost to this malware [56]. Huang et al. found $16m in criminal revenue due to ransomware via cryptocurrencies over a period of 2 years from 2015-2017 [36]. These figures were confirmed in an independent study by Paquet-Clouston et al. [76]. Of course, the direct losses due to ransomware (e.g., lost data and systems, time to recover) may be one to two orders of magnitude higher.

The rise of cryptocurrencies has also enabled a variety of other cryptocurrency-related frauds. By combing through all of the US SEC (Securities and Exchange Commission) and CFTC (Commodity Futures Trading Commission) filings involving cryptocurrencies or ICOs (initial coin offerings – how cryptocurrencies are crowdfunded at their start), we found: $7.1m lost to Ponzi schemes and similar 'investments'; $52m lost to mining scams; $36.3m raised by fake ICO scams; $6m raised by fraudulent cryptocoins; and $5m raised by other fake cryptocurrency services.

These numbers are indubitably low. Vasek and Moore found $7.3m raised just by Ponzi schemes during a one year period in 2013–4 [97]. There have also been popular cryptocurrencies that were later found out to be Ponzi schemes; the Ponzi scheme masquerading as the currency Bitconnect had a market cap of over $2.6 billion before falling to almost nothing in January 2018. However, it's unclear how much of that loss was borne by consumers (the Wall Street Journal estimated over $1bn). Another scam coin, OneCoin, raised over $90m in fraudulent profits just from Chinese consumers in 2016 [8] and IBCoin raised $8m from Taiwanese consumers in 2018–9 [20].

Pastrana and Suarez-Tangil looked at crypto-mining malware, programs run on victim machines which submit mining results on behalf of the criminals [77]. They found over a million crypto-mining samples had been in use over a 12-year period. They extracted the wallet identifiers and mining pool information and grouped the samples into campaigns. This allowed them to count the number of criminal groups involved and estimate their profits, Their conclusion was that at least 4.32% of the Monero crypto-currency had been mined by criminals, who had made a profit of around $56m over the entire period. The victims here have donated CPU cycles, and hence increased their electricity bills by a small amount as a result.

Cryptocurrencies have led to other crimes too, notably frauds by bitcoin exchanges and underground drug markets against their customers, as well as hacks against these exchanges and markets. Starting with the bankruptcy of Mt. Gox in 2014, where an exchange declared that a lot of its stock of bitcoin had been stolen and there were various allegations of internal malfeasance, there has been a whole series of exchanges and other traders using cryptocurrencies that went bust, often alleging hacks. Exchanges increasingly 'host' customers' bitcoin wallets – which means that the exchange controls the bitcoins rather than the customer, and operates more like a bank than a safe-custody service [6]. This leads to temptation; indeed the practice was pioneered by Mt. Gox prior to its collapse. A report by Chainalysis, a Bitcoin due-diligence firm, concluded that exchanges lost about $1bn to hackers in 2018, with most of the thefts perpetrated by two crime gangs; in addition to this, turnover on darknets where illicit goods such as drugs are bought and sold was $600m, approximately double the value for 2017 [19].

Finally, it is worth noting that the cryptocurrency markets themselves are being manipulated.

Gandal et al. [28] presented evidence that fraudulent bitcoin purchases initiated by the currency exchange Mt. Gox triggered bitcoin's price rise from $150 to $1,000 in 2013. More recently, Griffin and Shams [34] present evidence that suspiciously timed purchases of the Tether cryptocurrency may have propped up the price of bitcoin. While we cannot precisely quantify the extent to which price manipulations are driving cryptocurrency valuations, it seems reasonable to conclude that a significant portion of the $132 billion cumulative market cap for cryptocurrencies as of February 2019 could be a result of unlawful manipulation.

Putting a monetary estimate on the costs of cryptocrime is perhaps the hardest call in this paper. We're going to put forward $2bn, to account for the direct losses sustained as a result of exchange hacks and direct crimes against individuals by exchanges and others. If we were trying to increase the total, to argue for regulation, we might try to include market losses since the bubble burst, or at least market losses that result from investors losing confidence following scams, or once regulators cut manipulation. If we were trying to minimise the losses to argue against regulation, we could argue that if someone bought bitcoin for $1,000 and the value shot up to $100,000, whereupon they put the bitcoin in Mt. Gox and it got stolen, then they really only lost $1,000 rather than $100,000. But although some of us argue for greater regulation [6], this paper is not the place for that, and we steer a middle course. We also ignore indirect costs as they are too complex. Perhaps it is even a social good to puncture a bubble, especially one that contributes massively to CO_2 emissions. Again, this paper is not the place for that argument.

3.5 Fraudulent marketing

Fraudulent marketing can be divided into two categories: frauds aimed at advertisers who are selling legitimate goods but whose ad budgets are stolen, and ads (or search engine optimisation) aimed at selling non-existent, dubious or downright criminal products. We will deal with these in order.

Ad Fraud

Billions of dollars annually are spent on online advertising, but there's little authentication to verify that the users are actually viewing the ads that the advertiser is paying for. Because of this, there has been a steep rise in ad fraud corresponding to the rise in the price of Internet advertising. This fraud is usually in the form of an automated browser viewing ads, especially expensive video ads, whereupon the publisher pockets the revenue ('impression fraud'). There are a number of ways to measure ad fraud, similar to what we have discussed previously: the estimated amounts the criminals raised and the amounts that the advertisers lost by selling ads that were never seen by humans. We will report the second, though it's estimated that for every dollar that people running ad fraud make, the advertiser spent 2–5 dollars to serve those ads.

There was $36m lost from ad fraud during 2014–2018 via just two different campaigns from a single advertiser [91]. The amount lost to the entire industry was much higher, though harder to quantify directly. The same firms working with the FBI estimated that one of the campaigns cost advertisers approximately $3–5m a day [98]. This same campaign used no botnet-controlled computers, but rather used 850,000 IP addresses, corresponding to 1,900 servers under complete control of the criminals. Using pricing data from the datacenter in Dallas the criminals used, this adds up to around $2m per year in server costs for the criminals.

Ad fraud – including 'click fraud', 'impression fraud', 'traffic laundering' and other sorts of nefarious actions – has been contentious for many years because of the inherent conflict of interest

between advertisers and ad networks, and the difficulty for outsiders of doing any independent assessment of the ground truth. Our guesstimate would be that the losses are in the low billions per year worldwide.

Unlicensed and patent-infringing pharmaceuticals

In 2012, unlicensed pharmaceuticals were probably the goods most widely promoted using criminal advertising, accounting for roughly 80% of all spam email in 2010 [85, 57]. In our survey then, we reported that the Rustock botnet sent about a third of the world's spam, while promoting patent-infringing Viagra; they cost the industry perhaps $300m in spam filtering, yet made about 1–2% of that in revenue [47, 48]. Other analyses looked at higher-margin sales and placed overall pharma revenues in the high tens to low hundreds of millions worldwide [59, 51]. Last time, we allowed the more generous estimate, and put global criminal revenue at $288m. Pharma's market share now appears much diminished; the patents on Cialis, Levitra and Viagra has recently expired or are about to, and Viagra is available as an over-the-counter medicine at under $1 a pill. Unsolicited bulk email still imposes large costs via anti-spam and content filtering products and services, as well as risks of fraud related to the products now being promoted.

Coupon and loyalty-program fraud

With the rise of underground markets, operators have extended their drugs and pharmaceutical offerings with a more diverse set of products including coupons and loyalty program accounts, and this is evidenced by a large volume of offerings in underground markets. This type of crime comes in all sort of flavors such as making multiple copies of a coupon or forging a new discount voucher. Wegberg et al. studied more than 1,293 different coupon-related offerings sold in these markets during 2011 to 2017 with a total revenue of around $753,000 [96]. At the other end of the scale, an industry source estimates that coupon crime costs between $300m and $600m per year in the US alone [87].

Once more, the costs to the affected businesses and the costs to society are much larger than the crime proceeds, but are hard to estimate. A single seller in a single market place offered more than 2,000 $50-value coupons at one cent. If all the fake offered coupons had been used, and had displaced fully-paid sales, businesses would have lost $100,000. If they generated new sales, the loss would have been the marginal cost of production, which would have been much lower, especially for information goods.

Together with coupon crime, loyalty-program fraud is also on the rise [12]. Recent analyses of underground markets showed that travel/hospitality businesses and rewards programs collectively make up 13% of the types of account for sale. Moreover of all US non-card present fraud that occurred in 2016, 4% of attacks were on loyalty and rewards points accounts, but that number jumped to 13% in 2017 [12]. Roughly estimating the equivalent over the total losses reported on account takeover fraud [44], loyalty programs cost around $235m worldwide. Beyond the direct costs to the companies offering such programs, this type of fraud also incurs reputation damage and customer churn. According to a 2017 report by Experian, 26% of customers who fell victim to loyalty program fraud will cancel their rewards membership, 17% will stop doing business with the company and 37% will tell others about their loss and the vulnerability of the loyalty program [64]. So the indirect cost may be non-negligible. In any case, there is some overlap between loyalty-program fraud and our next category, namely travel fraud.

Travel fraud

A major fraud ecosystem to emerge since 2012 is travel fraud, and more specifically the sale of fraudulently obtained airline tickets. These are often sold via spam and search-engine optimisation, although there are reports of links to specific customers such as smugglers and people traffickers [38]. In any case, enforcement is made more complex by the fact that while some of the customers who buy deeply-discounted tickets know that they are illicit, not all do.

Accounting for losses is made harder by the variety of techniques used to obtain them. If they are bought using stolen credit cards, the losses end up in the banking industry, in the card-fraud figures presented above. If they are obtained by crooked staff at travel agencies or the travel departments of major firms, then these companies bear the cost. If they are obtained by manipulating airline reservation systems, or by airline insiders, the airlines carry the cost – which to them is lower, being essentially the tax component (as the operating costs per route are almost fixed). If they involve hacking customers' air miles, then customers may bear some of the losses while airlines may bear some when they make customers good, plus indirect costs due to brand damage, as mentioned in the section above. All that said, the best current estimate of the takings from airline fraud is $1bn a year [37].

Copyright-infringing software

The for-profit sale of counterfeit software, as with pharmaceuticals, depends on advertising. As the costs of online distribution are negligible, criminals' costs are email spam, search engine optimisation, and so on. The trend is downwards. In 2004, a survey commissioned by the Business Software Alliance found that 20% of UK respondents had purchased such software. By 2011, a study estimated that three of the top five leading counterfeit software organizations together made only about 37,000 sales per month [48]. If the average software sale was $50, then this reflects an annual turnover of only $22m worldwide for these organizations. Between 2004 and 2011, Microsoft's Office fell in price from hundreds of dollars to tens, and free software had become ubiquitous, so this was not surprising. Since then we expect that the software piracy business has languished still further, given the move to advertising-supported cloud services, and given that Android has displaced Windows as the world's dominant operating system.

Copyright-infringing music and video

Much the same applies to copyright-infringing music and video. There were vociferous disputes about music piracy in the early 2000s when Napster was taken down and the early file-sharing systems such as Kazaa proliferated in its place. That peaked about 2008 after which market power started to pass to platform owners such as Apple and Google. By the time of our 2012 paper, the criminal gains made directly by operators of downloading hubs were only in the hundreds of millions; for example, the raids on the Megaupload gang in Auckland, who were claimed to be the world's largest, led to asset seizures of about $50m [24]. By then, we estimated that they had roughly a third of the market and that the $50m represented a year's profits, giving a global figure for proceeds of crime of $150m.

This must have fallen substantially since then, as the platforms have consolidated their hold on music distribution. Apple, YouTube, Amazon and Spotify have displaced the music majors, and the subscription or advertising models have largely displaced the model of paying per CD or per track. Meanwhile Netflix has assumed a dominant position in movies, and computer games are even larger in terms of sales; again, subscription models have marginalised infringing downloads.

3.6 Fake antivirus and tech support scams

In our 2012 paper we discussed the fake antivirus products that had recently been studied by Stone Gross et al. [84] who had obtained access to sales databases and determined that three large groups were earning $97m per annum between them. In 2016 Nelms et al. [66], monitored socially-engineered downloads of various types of malicious malware on an academic network – finding that fake antivirus made up less than 1% of the samples. They attributed this low level of incidence to better awareness and to several police actions in 2011 that significantly disrupted the processing of credit card payments made for fake antivirus [50]. The 2018 IC3 Annual Report shows this category reduced to just under three thousand complaints with losses down to $7.1m [39].

The basic scam – being scared into purchasing software that at best does nothing and at worst leaves your computer open to other attacks – has not gone away. It has mutated into so-called 'tech support' scams involve telephone calls that purport to be from an ISP or often from Microsoft. The caller explains (mendaciously) that they have detected some sort of problem with the victim's computer and tries to pressure-sell some software to fix it [62]. The IC3 has published a detailed account of the scam, along with a number of variations [40], and their 2018 Annual Report [39] shows that they received over 14,000 complaints over the year relating to victim losses of $38m, an increase of 161% year on year. The IC3 notes that most of the victims were over 60 years old.

3.7 Compromised email accounts

In 2012 we discussed the 'stranded traveller' scam whereby an attacker who had compromised an email account posed as the account owner, explained some predicament in a foreign land and asked to be sent money to get home again. The ubiquity of mobile phones which allow rapid debunking of the story has pretty much put paid to this particular scam, so compromised email accounts are of limited use apart from for sending spam.

At least one enterprising criminal group mined the address books and 'sent email' folders of the accounts they had compromised and ever since then they have been sending email spam to the correspondents of those who were compromised long ago, forging the sender to be the compromised account – clearly hoping this will increase the chance of the spam being read.

In 2016 Onaolapo et al. [73] investigated what attackers did with a set of 100 accounts, and found that most uses of their deliberately leaked credentials were benign – they classify the attackers as merely 'curious'. However, around a quarter of accesses involved searches looking for exploitable emails such as correspondence from banks or bitcoin exchanges.

Since email accounts continue to be compromised at a very significant scale in a variety of different ways it hard to put a monetary value on the damage. However, the case of Yahoo gives some indication. In 2014 around 1 billion accounts were compromised by, the FBI alleges, hackers working for the Russian security services [92] and it was then discovered that in an earlier (so far not understood) attack all of Yahoo's 3 billion accounts were compromised. A settlement for a class action brought on behalf of 200m US and Israeli users awaits court approval. The proposed settlement will provide two years of credit monitoring and a contribution towards any costs incurred by users if they actually suffered any 'identity theft'.[6] The sum of $117.5m is reported to be involved (with a big chunk of that going to the lawyers who have pursued the class action) [14]. The size of such a settlement was a factor in the $4.8 billion sale of Yahoo

[6]The US records a lot of online crime using this term; see Section 5.1 below.

to Verizon, with $350m being knocked off the sale price when the breaches came to light [31]. The discount was in exchange for Verizon taking on half the costs of any future lawsuits. In addition to any civil lawsuits the US Security and Exchange Commission fined Yahoo $35m [94] and various other regulators have imposed fines such as the £250K fine in the UK [90].

3.8 'Fake escrow' and other fake companies

In 2012 we discussed 'fake escrow' websites which defraud people attempting to purchase cars, boats and motorcycles by pretending to provide shipment of the vehicle to the purchaser along with an escrow arrangement so that the victim is prepared to pay up front without sight of the merchandise. We provided a rough calculation of losses at $200m per annum.

This type of fraud continues but the data are too patchy to say whether it is increasing or decreasing. In January 2018 the FBI issued a general warning about online vehicle sales, citing 26,967 reports to IC3 over 41 months for a total victim loss of $54m [27]. There are more specific reports as well, for example, the Better Business Bureau (BBB) warned about a gang whose websites were easily grouped together – with the loss per victim being a four figure sum [11].

There are many other scams whose basis is a website describing a non-existent company.

For example, the majority of the websites offering pedigree puppies for sale are believed to be fake, and the victims pay not only for a non-existent puppy but also for its air transportation and then further expenses when the puppy is said to be stranded at an intermediate airport without food or water [9].

There are fake courier companies and fake shipping companies running scams that range from asking for customs fees for non-existent low-value gifts or prizes, to sophisticated scams involving shipment of cargoes of raw materials. Figures for losses are, as ever, hard to find and are very likely to exclude low levels of loss where people write it off to experience.

There are however some figures relating to the use of fake checks – a mechanism used in many scams – with the victim cashing the cheque and then forwarding some part of the proceeds to the criminal before realising that the cheque is fake and will not be honoured. The BBB has set out a very wide range of scams that use fake cheques in an October 2018 advisory, observing that there were 30 thousand reports made to IC3 in 2017, an increase of 12% year on year [10]. The potential for loss is significant – the Postal Inspection Service reports stopping fake checks with a face value of $62 billion from entering the United States in fiscal year 2017 [93]. Crime proceeds may be two orders of magnitude lower, though; the typical scam may involve a victim being recruited for what seems like an affiliate marketing scheme and being asked to remit proceeds, less commission, to head office. We do not have any robust figures but our best guess would be that such scams net in the tens of millions worldwide.

There are also fake banks, fake law firms and fake accountants whose websites exist as window dressing for complex scams involving large sums of money that are being smuggled out of the country, donated to charity, or inherited from a distant relative, as we shall now discuss.

3.9 Advance fee fraud

Advance Fee Fraud (AFF) is sometimes called '419 fraud' after the relevant article of the Nigerian criminal code. It comes in a large number of formats, from the deceased dictator's family who want to smuggle millions of dollars, to scams where people win millions in lotteries they have never entered. The common feature of all of these frauds is that the victim must pay out a

small amount of money (a tax, a bribe or just a bank account opening fee) in the expectation that this will release the large sum to them. If they pay out once then some other obstacle will arise and they will need to provide another advance fee – in extreme cases until they are personally bankrupt, or if they are re-purposing their employer's funds, until their own fraud becomes apparent.

There are very strong links historically between AFF and West Africa, particularly Nigeria, going back to the days when it was conducted by letter and then fax. Email has made communications simpler, although the higher-value scams often involve face to face meetings, and occasionally even kidnapping – so at the top end, this is not purely a cybercrime.

In 2012 we observed that data on losses was hard to come by and this has not changed since then. Although large losses occasionally make the news we continue to believe that most of these frauds involve sums under $1,000 and we see no reason to believe that total losses have changed all that much.

The most striking change since 2012 has been the change of focus by many of the West African fraudsters from targeting individuals to targeting businesses in 'Business Email Compromise' scams. We discuss this next.

3.10 Business Email Compromise

Business Email Compromise (BEC), also known as "man-in-the-email" or the "CEO scam" is a type of social engineering scam that occurs over email and that has grown rapidly since 2012, when we did not record it separately. When it affects individuals, often in the context of real estate transactions, it may be called Email Account Compromise (EAC). These scams can involve other cyber-criminal activity such as computer intrusions or account takeovers. Most BEC scams involve Nigerian criminal networks based in West Africa, but operating globally, where they secure bank accounts (often in Asia) to receive the victim's money.

A typical BEC scam starts with a fraudulent email message being sent to a company's financial manager, comptroller, or someone else with authority to execute wire transfers. The email falsely claims to be from the CEO or other person of authority within the company and instructs the receiver to initiate a wire transfer to a foreign bank account under control of the criminal.

BEC operators use three approaches to deliver the fake email to the victim. In most cases they purchase a domain name that is similar to the victim company domain name and create an account on this domain that matches the CEO's account. In other cases, they use malware to infect the victim's computer and send fraudulent emails directly to them. Lastly, they may use a spear-phishing attack to gain direct access to the CEO's email account.

Higher-value scams involve intercepting genuine invoices and sending replacements to accounts departments, with changes to the banking details so that monies are paid to a bank account controlled by the criminals. Lower-value scams typically involve a member of staff being inveigled into purchasing a few hundred dollars' worth of gift cards (perhaps under the pretext that the CEO will be distributing them as a staff bonus) and sending the details to the criminal who can then cash them out.

BEC schemes are successful because they prey on the victim's instinct to respond quickly to a request from a person of authority within their company. They are simple to execute and do not require a great deal of technology, capital or other resources. In spite of the relative ease of carrying out these attacks, their economic impact can be profound. The FBI's Internet Crime Complaint Center (IC3) has been publishing data on BEC/EAC since 2014,[7] and it is obvious

[7] `https://www.ic3.gov/media/annualreports.aspx`

from their data that this is a significant and growing problem. Here are their totals for frauds against US businesses and individuals:

year	loss (dollars)	complaints
2014	226 000,000	2 417
2015	246 226,016	7 837
2016	360 513,961	12 005
2017	676 151,185	15 690
2018	1 297 803 489	20 373

As for the global total, in June 2018 the IC3 estimated the accumulated total worldwide losses since 2013 to have reached $12.5bn from 78,617 incidents [41]; Trend Micro had estimated them somewhat lower in 2017 at $9bn [88].

These figures measure gross losses; however, banks are getting better at detecting BEC-related transactions, and in some cases may stop or revert them. Therefore, the net direct losses are more likely between 50% and 75% of the gross figures. This should not be confused with banks compensating victims among their retail customers (see Section 5.6), where the funds are not recovered and thus the financial loss is just shifted to a different party.

3.11 PABX and other telecoms-related fraud

The Communications Fraud Control Association (CFCA) publishes data on fraud losses associated with telephony, both fixed and mobile. Their methodology is to survey experts from within the industry as to what proportion of turnover is lost to fraud, and – with some statistical adjustments to account for company size – thereby estimate the size of the problem.

In our 2012 paper we had their 2011 results to hand – a headline global telecoms fraud figure of $40bn. Lots of this fraud was not cyber related ('subscription fraud' is just a term for the bill not being paid) but $4.96bn was 'PABX fraud' resulting from criminals reconfiguring a company's telephone system (Private Automatic Branch Exchange) to accept incoming calls and relay them onward. The latest report (for 2017 [21]) estimates the headline figure to be down to $29.2bn, with a fall of 23.2% from 2016. They attribute a lot of this reduction to structural changes (VOIP calls are cheaper so failing to pay for them is a lower loss!) but they also suggest that the cost of dealing with "cybersecurity issues" is rising.

PABX fraud is now down to $3.88bn, split half and half between traditional PABX installations and VOIP devices. Whereas in 2012 PABX fraud was still associated with the criminals selling access to allow expats to call home, the calls are now mainly to premium rate numbers both domestic and international. PABX access is now being exploited more imaginatively and some enterprising criminals are reprogramming voice recordings to say "Yes, I will accept the charges for a call to Zaire". However, just as we observed in 2012 the figure needs some caution since the CFCA does not set out whether this is the wholesale or retail cost of the calls – defrauded companies can often renegotiate the actual payment they make to settle their unexpected bill.

A number of other categories of telecoms fraud are cybercrime-related: account takeover (including by 'phishing') accounts for an estimated $3.1bn worldwide and the CFCA estimates a worldwide loss of $0.6bn for "denial of service attacks" – though no details are provided as to how this loss came about.

3.12 Industrial cyber-espionage and extortion

Around the time of our 2012 report, government spokespersons were talking up the risk of espionage and 'IP theft', particularly by China. This narrative continues, particularly in the context of the trade war between the USA and China. In 2012, we did not allocate a financial loss to these claims, because of the lack of evidence. While we do not dispute the occurrence of IP infringement, we failed to find any case with quantifiable losses where a drug company could not file a patent because of unauthorised prior disclosure, or any major software copyright infringement cases brought by western tech firms against Chinese competitors. This situation appears to be unchanged.

Our 2012 report also dismissed claims in a Detica report of £2.2bn lost annually to extortion, as the cases reported then (such as against online casinos) had substantially lower losses.

Here, we do have some significant recent losses to report, not just from ransomware but from worms masquerading as ransomware – specifically Wannacry and NotPetya. These both present as ransomware, but there is no mechanism for the authors to selectively decrypt the files of victims who pay up, and so such attacks are best classified as destructive denial-of-service attacks.

Wannacry, which was attributed to North Korea, infected a number of organisations worldwide, ranging from Taiwanese chipmaker TSMC (which cost a three-day outage) to the UK National Health Service, where five hospitals and a number of smaller clinics were affected, costing £94m.

NotPetya, which was attributed to Russia, was used to attack the Ukraine and collateral damage included the Maersk shipping company which was infected via its office there, leading to the replacement of much of its IT which, together with compensation to customers, cost $200m [58].

Large claims have been made for the overall damage caused by these two worms (both of which used stolen NSA exploits) but we might believe a total figure in the range of $1–2bn. For example, the losses to TSMC were initially reported as $255m in the security press but later, in the semiconductor trade press, the cost of the three-day outage was set at a 1% cut in gross margin for the quarter, which amounts to $84m [83]. The NHS figure is from the UK National Audit Office and is thus credible [65].

It is interesting to note that Mondelez' $100m insurance claim made for damage caused by NotPetya has been disputed by Zurich Insurance, who says it was an act of war [55]. However, that did not mean that the damage claimed for was illusory. The dispute will be decided by the courts. (We discuss cyber insurance as a data source in Section 5 below.)

Most crimes by states are much harder to tie to a clear financial loss. On May 13th 2017, hackers broke into Equifax and helped themselves to the personal information of at least 145.5 million Americans before the intrusion was reported on July 29. Executives sold stock before they notified the public on September 7th; Congress was outraged, and the CEO was fired. Analysts suspect that the beneficiary was a nation-state actor, as no criminal use has been made of any of the stolen data [69].

3.13 Fiscal fraud

In our 2012 report, we noted that both tax fraud and welfare fraud in the UK would count as computer crime under the EU definition from 2013, as almost all tax returns were online and all welfare claims would be from 2013. Much the same holds for many other countries. For developed countries we do have reasonable estimates of the amounts; for example about 0.8%

of welfare claims are bogus, with rates varying from under 0.1% for the state pension to over 4% of means-tested benefits. That adds up to a tad over $1bn. Figures for tax fraud are more slippery but were believed to be about 2% of the tax take, or ten times as much as welfare fraud; we settled on $12bn for the UK alone.

On top of this vast sum is a much smaller sum in third-party tax fraud, such as criminals impersonating citizens by electronically filing fraudulent tax returns. In 2012, we cited IRS estimates from 2010 to the effect that $5.2bn was stolen via around 1.5 million such tax returns [3]. The IRS has suffered significant declines in resourcing and criminal prosecutions since then, but has claimed $9.69bn tax fraud identified [43]. The General Accounting Office also noted that fraudsters used false identities to steal at least $1.68 billion in tax refunds in 2016 [29].

3.14 Other frauds and scams

Many other categories of fraud and scam have been reported in recent years, involving both business-to-business and business-to-customer transactions in just about every kind of economic activity from auctions to travel. Some of these relate simply to non-existent services sold online, an example being accommodation fraud where crooks advertise apartments to let and collect deposits; we estimate the takings from this in the UK to be £5–7m pa. Others involve some more subtle exploitation of technology; for example, travel fraud can involve manipulation of airline booking mechanisms as well as the more straightforward techniques of buying tickets using stolen credit cards or having them bought by corrupt insiders in travel agencies. Others involve abusive competition; companies that sell through Amazon may find their competitors attacking their sites by filing spammy reviews, causing their products to be suspended on suspicion of abusive marketing, and be forced to go through lengthy appeal processes to reinstate their business. We have no figures for the financial costs of abuses of this kind.

Some frauds may net relatively modest amounts of money but do disproportionate emotional damage. According to the Federal Trade Commission (FTC), romance scams are on the rise. In 2018, the FTC's online database of consumer complaints, the Consumer Sentinel, recorded over 20,000 reports of romance scams, which cost victims $143m. That's up from 8,500 reports in 2015, which amounted to $33m in losses. Last year, the median individual lost roughly $2,600, which according to the FTC, is roughly seven times higher than other types of scams.

Cybercrime researchers, trade associations, credit card issuers and others spend increasing amounts of time investigating a multitude of online scams, while other scams are still ignored as no capable actors are sufficiently motivated to do anything. So rather than diving down into still more detail here, we will return later to consider victimisation studies. These studies assess crime not from crime reports but from surveys of a representative sample of a population who are asked whether they were victims of a crime last year. These surveys give us the closest we have to ground truth, and as we will see, they paint a depressing picture.

3.15 Summarizing the summaries

Having presented a lot of information in this section, we summarise the main categories in the following table, giving representative figures (not always for the same geographical areas) and an indication of what's changed since 2012.

	crime type	value	changes since 2012
§3.1	Online credit card fraud	£731.8m (UK)	reduced percentage of turnover
§3.2	Online bank fraud	£121.4m (UK)	increased, but more activity
§3.2	Authorised push payments	£236m (UK)	a new category since 2012
§3.3	In-person card fraud	£158m	has grown but may have peaked
§3.4	Ransomware	well over $10m	much increased since 2012
§3.4	Cryptocrime	$2bn	was not an issue in 2012
§3.5	Ad fraud	low $billions	increased, but no good public data
§3.5	Pharmaceuticals	tens of $millions	reduced since 2012
§3.5	Coupon fraud	$300m+ (US)	not discussed in 2012
§3.5	Loyalty-program fraud	$235m	new since 2012
§3.5	Travel fraud	$1bn	new since 2012
§3.5	Counterfeit software	low $millions	decreasing trend of 2012 has continued
§3.5	Copyright theft	low $10 millions	fallen substantially
§3.6	Fake antivirus	$7.1m (US)	down by 90% since 2012
§3.6	Tech support scams	$39m (US)	growing very rapidly
§3.7	Compromised email		regulatory & legal costs now dominate
§3.8	Fake companies	tens of $millions	few good figures
§3.9	Advance fee fraud	low $100 millions	no reliable estimates
§3.10	Business email compromise	$1.3bn (US)	see APP for related UK figure
§3.11	Telecoms fraud	$7 billion	markedly down since 2012
§3.12	Wannacry / NotPetya	$1–2 billion	one-off events, so may not recur
§3.13	Fiscal fraud	many $billions	tax fraud, welfare fraud, etc.
§3.14	Romance scams	$143m (US)	more reports than in 2012

4 The Infrastructure Supporting Cybercrime

We now review the infrastructure supporting cybercrime, such as botnets. These are used to enable lots of different crimes, so we estimate their costs separately to avoid double counting.

4.1 Botnets

Cybercriminals continue to use networks of infected computers – so-called botnets – to support their operations. In recent years, the 'Internet Of Things' (IoT) has facilitated the spread of new botnets, an example being the Mirai botnet that infects devices such as CCTV cameras and DVRs that have known default passwords. This has lowered the acquisition costs of 'botnet herders' who can now build large botnets of IoT devices within days. Moreover, the proliferation of cybercrime markets has opened doors for the inception of new botnet business models, supporting a range of criminal services.

In the beginning, botnets were mostly used to send spam. Today cybercriminals have managed to monetize botnets in multiple ways: they can distribute a range of scams or even ransomware; perform DDoS attacks; mine cryptocurrencies; or be used to cheat advertising networks or social media. The botmasters' turnover can vary significantly depending on the botnet type and monetization strategy. For instance, while a banking botnet was used to steal more than €36m from 30,000 bank customers during 90 days [46], a DDoS-for-hire botnet only earned its herder some $26,000 per month [15]. In fact, in 2012 our best estimate of the botnet herders' revenue

was not large enough to make it into our summary table. However many of the crimes they support, such as spam and click fraud, are of real consequence.

The costs of botnets thus falls not only on Internet intermediaries and their customers but also on society as a whole. Previous works [7, 18] have shown that almost 85% of the botnet infrastructure is located in consumer ISP networks. The remaining machines include the part of the infrastructure that is used to control the bots and are typically placed in hosting centres. However, not all providers suffer the costs of botnets equally. Mimicking the market structure, the concentration of bots across ISPs follows a power-law distribution [7], i.e., two or three ISPs typically account for over half the total infected machines within a country.

In order to fight botnets, medium-sized and large-sized ISPs have set up abuse handling departments. Their costs of these are mainly driven by the salaries and benefits for abuse desk responders plus their technical support staff and managers. On top of staff costs, these departments must bear technology and telecom expenses (computers, software licensing fees, etc.), facilities costs (office space, utilities, insurance, etc.) and training costs too. A recent survey quantified the average cost of a handling a ticket at $15.56 plus $1.60 per minute of handling time [82]. Thus a typical European ISP with about 5 million subscribers that opened 200,000 abuse-related tickets in 2018 will spend over €3m.

To alleviate these costs and make abuse handling affordable to small ISPs, different national and European initiatives have emerged. For example, *abuse.io* an open source abuse-management system that automatically parses incidents into abuse tickets; sends automatic notifications; and allows abuse desks and end users to reply, close or add notes to the ticket. At the European level, with a total cost of €15.5m, the Advanced Cyber Defence Centre (ACDC) [2] was established in 2013 to provide a complete set of solutions accessible online to mitigate on-going attacks and targeted both to end-users and to network operators. Similarly, an Abuse Information Exchange (a.k.a AbuseHub) [1] was set up in the Netherlands in 2014 to effectively share and use information on botnet infections and other internet abuse by centrally collecting, analyzing and correlating information from various national and international sources. While these initiatives do not cover all types of abuse, they do significantly reduce the costs of handling abuse events by providing automation.

4.2 Botnet mitigation by firms

Botnet mitigation by firms other than service providers (and banks, whose anti-fraud measures we account for above) is hard to nail down, as are figures for the total information security industry. Some reports available in 2012 suggested of the order of $20bn [17], while we now have a Gartner report claiming that the total information security spend worldwide is about $100bn, with half of that going on services [30]. Again, much of this is compliance, including everything from PCI DSS audits to internal controls aimed at providing assurance on governance. Much of the rest would be necessary even if cybercrime were to cease, from identity management to salaries of sysadmins who do things other than security. So how can we measure the risk-reduction components?

In 2012 we estimated the global antivirus business at $3.4bn, scaling from Symantec's 2011 sales of $6.2bn; these grew to only $6.55bn by 2015, so growth isn't spectacular. The second-largest firm, Avast reported annual sales of $714m in 2016–7, while Trend Micro had Q4 sales of $375m in 2018. Overall an estimate of $4bn seems reasonable. Anti-virus software isn't the whole story, of course; firms also get DDoS defence services from Cloudflare. There's also the global cost of software patching, which we estimated at $1bn in 2012. Then, we were cautious and ascribed a

global figure of $10bn to generic cybercrime defences by companies worldwide. This strikes us as probably still about right.

As for IoT botnets such as Mirai, the appropriate countermeasure is probably a law on patching, such as the new EU directive on sale of goods (2015/0288) which when it comes into force will require firms that sell goods with digital elements to maintain those elements during the lifetime that consumers can reasonably expect. This will impose substantial costs on some firms, but software patching is good practice and needed for product safety and functionality in any case, and we are reluctant to describe compliance with consumer-protection law as a cost of cybercrime. A similar argument applies to the bug bounty programs used to incentivize discovery and reporting [100]. Their costs are smaller than patching, even though their administrative costs tend to be larger than the bounties themselves. (This costs imbalance persists even when part of the administrative effort is outsourced to a platform.)

4.3 Botnet mitigation by consumers

In 2012, we noted two robust and independent estimates that a little over one million British households have had a machine in a botnet at least once per year: one from Microsoft, whose Malicious Software Removal Tool cleaned up around 500,000 bots in the UK in the first half of 2010 [61, 60]; and a comparison by van Eeten of Dutch infection levels to those in the UK and other countries [95], which revealed that in 2010, around 6% of the 19 million UK broadband subscribers had a machine in a botnet at some point during the year. We guesstimated the costs of cleanup at $500 per infected household, or $30 for every household with a broadband connection. We also estimated from the Eurostat 2010 ICT survey that 88% of all households with a broadband subscription use at least one antivirus product. A conservative estimate would put the worth of a single license at $10, ignoring for a moment which actor bears this cost. For the UK, this would put the total cost of antivirus countermeasures at around $170m.

Unfortunately, Eurostat discontinued the relevant series in 2010, which stops us updating the figure. Yet with antivirus functions having been integrated in the Windows operating system since 2012, the need to buy additional products disappeared for almost all consumers. Hence, this component of defense costs might be lower today, as consumers increasingly understand that the security industry's sales tactics are based on myths. The closest approximation to the Eurostat question in 2010 is a related indicator in the 2014 Eurobarometer Special on cyber security, according to which only 50% of UK residents (and 61% for the EU28 as a whole) say they have installed antivirus software in response to concerns about security issues.

4.4 Other botnet mitigation costs

We noted in 2012 that the US spends about $100m fighting cybercrime at the Federal level (FBI, Secret Service, FTC and NCFTA) and we assumed the same again at state level. The US is by far the major player in cyber enforcement, and seems to do about half the work; so we estimated global law-enforcement expenditures at $400m. For example, we estimated the total UK police cyberbudgets at only $15m a year. The overall picture here seems unfortunately to be little changed.

4.5 Pay-per-install

In our 2012 paper, we cited Caballero et al. showing that 12 of the world's top 20 malware families used PPI services for distribution [16], and by Wondracek et al. exploring the porn

industry's contribution to PPI [99]. However the prices per infection ranged from 5¢ per machine in the USA down to fractions of a cent in less developed countries, so even if we assume 100m machines are infected every year and half of these done by PPI firms at an average cost of $50 per thousand, that's $2.5m – which lay below our reporting threshold. If anything, botnet recruitment seems to have become easier in the seven years since, because of the large numbers of vulnerable connected IoT devices that are trivially recruited, as exemplified by the Mirai botnet.

5 New Perspectives

In our 2012 paper, we scaled UK estimates up to global ones and vice versa using the rule of thumb that Britain's GDP is about 5% of world GDP, and presented them in a table. We warned that 'it is entirely misleading to provide totals lest they be quoted out of context, without all the caveats and cautions that we have provided'. Yet journalists happily ignored this and simply added up the columns, proclaiming large headline figures for global cybercrime – which were essentially twenty times our estimate of UK income tax evasion, as this was the largest figure in the table.

The most interesting things we have discovered while preparing this perspective seven years later are what has changed. In section 3 we discussed how some cybercrime has changed (card fraud has doubled, but only because card transactions have; the fraud rate is actually down slightly) and how other cybercrimes have emerged (from travel fraud to ransomware and hacks against bitcoin exchanges) while other cybercrimes have tailed off (such as unlicensed pharmaceuticals).

Since our paper appeared in 2012, we have important new sources of data. There have also been several other studies seeking to replicate, extend or critique our methodology. However, the biggest change since 2015 is the availability of large-scale victimisation studies.

Such studies have been used in criminology for many years, as some crimes (such as rape) are significantly under-reported, and police crime reports do not therefore give an accurate picture. They typically involve asking a representative sample of some tens of thousands of residents whether they suffered a crime in the previous year, with questions on both violent crime and traditional property crimes such as burglary and car theft. Since our last paper, a number of countries have added questions about fraud and scams. The picture that emerges is that online property crime is now about half of the total. In some countries (like Britain) it's slightly less than half and in others (such as France) it's slightly more, and there are significant differences in precisely what questions get asked. But the big picture that emerges is that online crime is now half of all property crime.

5.1 The US identity theft studies

The US National Crime Victimization Study (NCVS) focuses on violent crime but has occasional supplements on identity theft, with the most recent covering 2016 [35]. This substantially covers unauthorised debits to credit cards and bank accounts, which were suffered by just over 10% of American residents in 2016, up from 7% at the last survey in 2014. About half were contacted by their institution about suspicious activity, and about half the rest noticed fraudulent charges or missing money. Only about a quarter knew how the compromise occurred. The great majority (88.4%) dealt with their bank and very few (6.8%) with the police. Most were made good; only 12% ended up out of pocket, and only 15% of these made substantial losses ($1,000 or more).

The main other aggravation was hassle; while most victims had the problem put right within a day or less, a minority took weeks to months and many of these suffered distress as a result.

In 2016, Tcherni et al. investigated whether cyberspace was hiding a crime wave [86]. They noted that the traditional property crimes on which the FBI gathers national statistics had been falling since the 1990s, while online card and other fraud had been increasingly organised since about 2004. To what extent might crime be simply moving online? They have an extensive discussion of the methodological problems in getting accurate comparisons; and in the case of large breaches, where millions of credentials are leaked, only a tiny proportion are actually used. In many cases, victims are made whole promptly, thanks to the USA's robust financial consumer protection laws. However, the NCVS, five-yearly surveys by the National White Collar Crime center, and a private victimisation survey by Javelin, all start to provide reference points – including (in the case of NCVS and Javelin) monetary losses. They conclude that the rate at which US residents are affected by online property crime now outstrips that of traditional property crime. They conclude that "criminologists would be wise to be circumspect before declaring that crime has dropped as radically as traditional measures appear to reflect".

5.2 The UK data

The British story is similar. In 2005, the UK government brokered a deal between the police and the banks whereby fraud was reported first to the banks, who in turn might report it to the police if they thought this appropriate. The banks also agreed to fund a specialist police unit to investigate card and cheque fraud. The public rationale for this was efficiency; the effect was to manage the fraud statistics downwards. For a decade, reported crime fell; successive police chiefs and Home Secretaries took the credit. Some criminologists complained that crime was just going online, where it wasn't being counted. Eventually in 2015 the Office of National Statistics included fraud in the UK victimisation study. It became rapidly clear that more than twice as many households were falling victims to scams (that are mostly online) than suffered traditional property crimes such as burglary or car theft.

The most recent (2018) findings give more solid data on the extent to which official bank figures underestimate the problem [71]. For the year ended September 2018, fraud is estimated at 3.5m offences and stable, being about equal in volume to theft; while computer misuse fell by a third to a million, making them about equal to criminal damage; adding in burglary, vehicle offences and shoplifting (at about 400,000 each) leaves online property crime slightly below the traditional variety. However the narrative that crime fell over the past ten years is now acknowledged to have been based on an illusion. The inclusion of fraud and computer offences has increased the total from about 6 million offences to about 11 million, and many of the graphs in the report have a discontinuity. Fraud was also experienced by more adults than any other crime.

5.3 The Belgian victimisation study

A big Belgian study [74, 75] surveyed 1000 people on victimisation in both 2015 and 2017, did two online surveys of Belgian businesses with about 300 responding, and did 160 face-to-face interviews. 16.5% of the population reported reducing or stopping certain activities online as a security measure, including 5.9% for electronic banking, 10.4% for online shopping, and 9% for social network sites. They noted that malware provides the most victims but scams provide the biggest losses. Their fraud figures are higher than many academic studies but below commercial scaremongers. They observed a decrease in the percentage of businesses reporting victimisation of at least one type of cybercrime (from 66.5% in their first survey to 53.6% in the second).

Only a handful reported serious losses; most thought other firms were suffering more damage than was in fact the case.

5.4 The French victimisation study

France has a victimisation survey based on face-to-face interviews with 16,000 households [70]. Fraudulent debits to bank accounts are stable after strong growth since 2010, at 1,219,000 households or over 4% of the total, while there were a further 1,712,000 scams of which 492,000 were other frauds and the rest ranged from entrapment and blackmail to online orders leading to faulty or non-existent goods. By comparison, burglary affects about 2% of households; a further 2% suffer vandalism and another 0.9% a theft that does not involve breaking in (mostly from the garden). Just under 1% suffered car theft, and just over 1% had a bike theft. A further 2% suffered nonviolent personal theft, such as pickpocketing, while just under 1% were mugged. Thus fraud and scams together amount for more offences than the rest of property crime. Fraud is growing strongly, having doubled since 2011 – and the only other property crime that's growing rapidly is nonviolent personal theft, thanks to smartphones. A third of victims reported the fraud to the police, mostly as a condition of getting reimbursement from their bank. Since June 2016 there has been an online police platform for victims to file such reports. Add to this the fact that of perhaps two million cases of threatening behaviour, 7% were made on social networks and a further 9% by phone.

5.5 The Australian victimisation study

13% of the 9,947 respondents to a 2017 Australian survey reported misuse of their personal data in the previous 12 months [32]; this survey also tried to quantify harm, and found that the victims' total financial losses were AUD 2.9m – more than double those in the previous year. This suggests losses per head of population in the low hundreds of dollars, rather than in the tens as we reported in 2012.

5.6 The E-CRIME cross-country victimisation study

The victimization study carried out by some of us [80, 81] in the context of the EU-funded research project "Economic Impacts of Cybercrime" (E-CRIME, 2014–2017) tried to implement the lessons learned from our 2012 paper. It covered a list of popular cybercrimes against consumers, asked about lost time and money, differentiating between losses before and after compensation from a third party, e. g., a bank in the case of online banking fraud. The data were collected in the summer of 2015 from six selected EU countries, using a "boosting" technique to increase the number of cybercrime victims in the sample. Another technique to increase the number of victims is to ask for cybercrime experience in the past 5 years (rather than 12 months). If a respondent has been victimized multiple times, the disambiguation method was to collect data for the "most severe" case, which likely is the one respondents remember best. The data is representative (to the extent possible at the current state of the art) for each country by applying inverse probability weighting in order to adjust the over-sampling bias. The higher number of victims (with lower weight) reduces the standard errors of estimates and allows more precise measurements than secondary analyses of the other victimization studies of which we are aware. Budget constraints limited the data collection to six countries and did not allow a second wave.

The results support the common conjecture that loss distributions are skewed to the right, and best modelled with a zero-inflated log-normal distribution: many victims report losing nothing, and only a few lose substantial amounts. Hence medians are significantly lower than means, and we may need more complex estimators to measure the overall impact.

The annual loss per person (not per victim) of crimes related to online shopping in less than €10. The figure is about twice as high for the initial loss of the three payment-related crimes studied, but drops to the same range after accounting for reimbursements by banks or other payment service providers. The reimbursement process is associated with a time loss of 8 hours on average. The worst type of crime from a victim's perspective are scams, which take more time and cost every citizen almost €20 per year, as there is no party who either responds to the crime or compensates the victim.

5.7 Development of the cyber insurance market

The market for cyber insurance has matured since 2012, reaching an estimated $4 billion in premiums in 2018, about double the size of 2015. In theory, cyber insurance could help mitigate risk, not only transfer it. However, there is little evidence of this happening so far. For our purpose, claims data provides some guidance for triangulating the direct costs of cybercrime.

Our best estimate for claim payouts is based on a NetDiligence report from 2015 [67], according to which 83% of the analyzed claims paid out a total of $75 million. Scaling this up from the 5% of the market that NetDiligence saw, the data suggests that the total payout is in the order of $1.5 billion or 75% of premiums, leaving a quarter for administrative costs and profits [13]. Note that this extrapolation is crude because it assumes that the self-selected sample is representative, but it is the best we could find. Assuming unchanged profitability, this suggests that $3 billion of direct costs to businesses are transferred to insurance carriers. These figures are primarily related to data breaches at smaller organizations ($<$ $2 billion in revenues) located in the US, where the market for cyber insurance is most developed. Some fraction of the cost is already accounted for in crimes discussed in the previous sections. Notably, a third of the total payout was for legal costs, chiefly defense lawyers and settlements, that are not covered by our previous estimates [68].

Cyber insurance develops in a symbiotic relationship with data providers that offer risk assessment to organizations seeking insurance and underwriters, such as SecurityScorecard, Bitsight, and QuadMetrics. Indeed it seems like Bitsight has become the new Standard & Poors.

6 Conclusion

Our 2012 paper concluded as follows:

> A final point is that, according to the British Crime Survey, some 2% of respondents reported suffering a traditional acquisitive crime such as burglary or car theft, while more than double that number suffered fraud. The survey did not disambiguate the online and electronic frauds of interest here from the door-to-door and boiler-house variety, but the former probably accounted for most of it. ... If this interpretation is correct, then cybercrime is now the typical volume property crime in the UK, and the case for more vigorous policing is stronger than ever.

We seem to have called that about right. Online property crime may be slightly less than half of total property crime in the latest UK survey by ONS and slightly more than half in France; the criminologists are arguing about the picture in the USA. However the claim by police forces and government officials that crime overall was falling was wrong; physical crime was falling while online crime was rising. The two are not simple substitutes; cause and effect are complex and globalisation plays a role. But it is not appropriate to ignore cybercrime simply because the losses are usually small in financial terms; this is the case for most street robberies and burglaries too. Victimisation can cause real psychological distress [63].

In terms of the amounts stolen by criminals, it is still the case that traditional frauds such as tax and welfare fraud cost each of us as citizens a few hundred pounds/euros/dollars a year, while payment card and online banking fraud cost each of us as citizens a few tens of pounds/euros/dollars a year. It is still the case that cyber-frauds such as fake antivirus net their perpetrators relatively small sums, with common scams pulling in tens of cents/pence per year per head of population, while the indirect and defence costs we pay, in terms of securing our systems, are much larger – in the tens of dollars a year.

What has changed, thanks to the victimisation studies, is our assessment of criminal earnings. In 2012 we wrote

> In total, cyber-crooks' earnings might amount to a couple of dollars per citizen per year. But the indirect costs and defence costs are very substantial – at least ten times that.

If 6% of us are victims of a scam with an average take of $200 then criminal proceeds are nudging their way into double figures. They may well have been there already in 2012; we just didn't have the data. The data are still not particularly robust (the Australian victimisation survey would put the losses in three figures rather than two).

Indeed, this study suggests ways in which our victimisation statistics could be improved. Several countries now ask questions about fraud and cybercrime in their general victimisation surveys, but they ask different questions, in different ways, and generally do not help much in assessing the direct or indirect costs of such offences. There has been no European survey since 2014; Eurostat should be doing annual surveys to give us a consistent picture, and such surveys should be extended to the USA, Canada and other major markets. If governments drag their feet, then we should consider academic / NGO surveys to fill the gap.

But even although we'd like to measure online crime better, it is still clear that the move of property crime from physical to online changes where the costs fall. Instead of the victim's costs exceeding the defence costs and criminal-justice system costs put together, the indirect and defence costs are now dominant. In effect, the cost of crime is being socialised. The law-enforcement community is making some progress, for example by getting better at pursuing crooks across national borders, but much remains to be done.

The core problem is that many cybercriminals operate with near-complete impunity. We concluded in 2012 that while we might perhaps spend less in anticipation of computer crime (on antivirus, firewalls etc.), we should certainly spend an awful lot more on catching and punishing the perpetrators. We see no reason to change this policy advice. We will not get a real handle on cybercrime until we put an end to impunity.

Acknowledgements

We thank Boris Hemkemeier for insightful comments on an earlier draft, Alice Hutchings for reviewing and commenting on the final draft, and Steven Murdoch for maintaining Figure 2 over the past seven years. Rainer Böhme's work on this topic is supported inter alia by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740558 (TITANIUM), the Austrian FFG's KIRAS programme under project VIRTCRIME, and Archimedes Privatstiftung, Innsbruck, Austria. Richard Clayton is supported by the Engineering and Physical Sciences Research Council (EPSRC) [grant number EP/M020320/1].

References

[1] AbuseHub. Abuse Information Exchange. https://www.abuseinformationexchange.nl/english.

[2] Advanced Cyber Defence Centre – Joining forces to fight botnet. https://www.acdc-project.eu/.

[3] Lizette Alvarez. With personal data in hand, thieves file early and often. *New York Times*, May 2012. http://www.nytimes.com/2012/05/27/us/id-thieves-loot-tax-checks-filing-early-and-often.html.

[4] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. Measuring the Cost of Cybercrime. In *Workshop on the Economics of Information Security*, 2012.

[5] Ross Anderson, Rainer Böhme, Richard Clayton, and Tyler Moore. Security Economics and the Internal Market, January 2008. http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec.

[6] Ross Anderson, Ilia Shumailov, Mansoor Ahmed, and Alessandro Rietmann. Bitcoin redux. In *Workshop on the Economics of Information Security*, 2018.

[7] Hadi Asghari, Michel JG van Eeten, and Johannes M Bauer. Economics of fighting botnets: Lessons from a decade of mitigation. *IEEE Security & Privacy*, 13(5):16–23, 2015.

[8] $45.7 million recovered from Chinese OneCoin scammers. https://behindmlm.com/mlm/regulation/45-7-million-recovered-from-chinese-onecoin-scammers/.

[9] Better Business Bureau. Puppy scams: How fake online pet sellers steal from unsuspecting pet buyers – a BBB study. https://www.bbb.org/article/investigations/14214-puppy-scams-how-fake-online-pet-sellers-steal-from-unsuspecting-pet-buyers-a-bbb-study, 13 Apr 2018.

[10] Better Business Bureau. Don't cash that check: BBB study shows how fake check scams bait consumers. https://www.bbb.org/article/news-releases/18367-dont-cash-that-check-bbb-study-shows-how-fake-check-scams-bait-consumers, 4 Oct 2018.

[11] Better Business Bureau, St Louis. Vehicle shippers springing up on internet may be scams, BBB warns. https://www.bbb.org/article/news-releases/17905-vehicle-shippers-springing-up-on-internet-may-be-scams-bbb-warns, 14 Jun 2018.

[12] Heidi Bleau. Loyalty Points Fraud: Why Reward Programs are a Growing Target. https://www.rsa.com/en-us/blog/2018-11/loyalty-points-fraud-why-reward-programs-are-a-growing-target, 2018.

[13] Rainer Böhme, Stefan Laube, and Markus Riek. A fundamental approach to cyber risk analysis. *Variance*, 12(2):to appear, 2019.

[14] Jon Brodkin. Yahoo tries to settle 3-billion-account data breach with $118 million payout. https://arstechnica.com/tech-policy/2019/04/yahoo-tries-to-settle-3-billion-account-data-breach-with-118-million-payout/, 10 Apr 2019.

[15] Ryan Brunt, Prakhar Pandey, and Damon McCoy. Booted: An analysis of a payment intervention on a ddos-for-hire service. In *Workshop on the Economics of Information Security*, 2017.

[16] Juan Caballero, Chris Grier, Christian Kreibich, and Vern Paxson. Measuring Pay-per-Install: The Commoditisation of Malware Distribution. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, Berkeley, CA, USA, 2011. USENIX Association.

[17] Canalys Inc. Enterprise security market to exceed $22 billion in 2012, December 2011. http://www.canalys.com/static/press_release/2011/canalys-press-release-201211-enterprise-security-market-exceed-22-billion-2012.pdf.

[18] Orçun Çetin, Carlos Gañán, Lisette Altena, Samaneh Tajalizadehkhoob, and Michel van Eeten. Let me out! evaluating the effectiveness of quarantining compromised users in walled gardens. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pages 251–263, 2018.

[19] Chainalysis. Crypto Crime Report, January 2019.

[20] Liu Chien-pang and Ko Lin. Over a dozen suspects arrested for cryptocurrency fraud, January 2019. http://focustaiwan.tw/news/asoc/201901260013.aspx.

[21] Communications Fraud Control Association. 2011 global fraud loss survey. http://www.cfca.org/fraudlosssurvey/, 2011.

[22] Cybersource. Masters of Balance – What it Takes to be a Fraud Management Leader. http://forms.cybersource.com/, 2019.

[23] Jim Eckenrode and Sam Friedman. The State of Cybersecurity at Financial Institutions, May 21, 2018. Deloittes.

[24] Clive Eliot. Kim Dotcom – Pirate or Enabler? http://www.nzherald.co.nz/auckland-region/news/article.cfm?l_id=117&objectid=10784190, 2012.

[25] European Central Bank. Fifth report on card fraud, September 2018.

[26] European Commission. Towards a general policy on the fight against cyber crime, May 2007. COM(2007) 267 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF.

[27] Federal Bureau of Investigation. Fraudulent Online Vehicle Sales. https://www.ic3.gov/media/2018/180117.aspx, 17 Jan 2018.

[28] Neil Gandal, JT Hamrick, Tyler Moore, and Tali Obermann. Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, 95:86–96, May 2018.

[29] GAO. Tax Fraud and NonCompliance GAO Report 224.

[30] Gartner. Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019.

[31] Vindu Goel. Verizon will pay $350 million less for Yahoo. *New York Times*, 21 Feb 2017.

[32] Susan Goldsmid, Alexandra Gannoni, and Russell G Smith. Identity crime and misuse in Australia: Results of the 2017 online survey. Australian Institute of Criminology Statistical Report 11.

[33] James T. Graves, Alessandro Acquisti, and Nicolas Christin. Should credit card issuers reissue cards in response to a data breach?: Uncertainty and transparency in metrics for data security policymaking. *ACM Trans. Internet Technol.*, 18(4):54:1–54:19, September 2018.

[34] John M Griffin and Amin Shams. Is bitcoin really un-tethered? Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066, 2018.

[35] Erika Harrell. Victims of Identity Theft, 2016. US Department of Justice NCJ251147, Jan 2019.

[36] Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Elie Bursztein, Kylie McRoberts, Jonathan Levin, Kirill Levchenko, Alex C Snoeren, and Damon McCoy. Tracking ransomware end-to-end. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 618–631. IEEE, 2018.

[37] Alice Hutchings. Flying in Cyberspace: Policing Global Travel Fraud. *Policing: A Journal of Policy and Practice*, 10 September 2018.

[38] Alice Hutchings. Leaving on a jet plane: the trade in fraudulently obtained airline tickets. *Crime, Law and Social Change*, 70(4):461–487, Nov 2018.

[39] IC3. 2018 internet crime report. `https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf`.

[40] IC3. Tech support fraud. `https://www.ic3.gov/media/2018/180328.aspx`.

[41] IC3. Internet Crime Complaint Center Public Service Announcement I-071218-PSA, July 12, 2018.

[42] Martin Innes. Signal crimes and signal disorders: notes on deviance as communicative action. *British Journal of Sociology*, 55:335–355, September 2004.

[43] Internal Revenue Service. Criminal Investigation 2018 Annual Report.

[44] Javelin Strategy & Research. Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study — Javelin. `https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new`, 2017.

[45] Carl Kalapesi, Sarah Willersdorf, and Paul Zwillenberg. The Connected Kingdom: How the Internet is Transforming the U.K. Economy. `http://www.connectedkingdom.co.uk/the-report`, October 2010.

[46] Eran Kalige and Darrell Burkey. A case study of eurograbber: How 36 million euros was stolen via malware. `https://www.checkpoint.com/downloads/product-related/whitepapers/eurograbber-malware-bank-customers-millions-stolen.pdf`, 2015.

[47] Chris Kanich, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, and Stefan Savage. Spamalytics: An empirical analysis of spam marketing conversion. In *Proceedings of the ACM Conference on Computer and Communications Security*, October 2008.

[48] Chris Kanich, Nicholas Weaver, Damon McCoy, Tristan Halvorson, Christian Kreibich, Kirill Levchenko, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. Show Me the Money: Characterizing Spam-advertised Revenue. In *Proceedings of the USENIX Security Symposium*, San Francisco, CA, August 2011.

[49] Akif Khan and James Hunt. UK Online Fraud Report 2012. `http://forms.cybersource.com/forms/FraudReport2012UKUKwebwww2012`, 2012.

[50] Brian Krebs. Fake antivirus industry down, but not out. `https://krebsonsecurity.com/2011/08/fake-antivirus-industry-down-but-not-out/`, August 2011.

[51] Brian Krebs. SpamIt, Glavmed Pharmacy Networks Exposed. Krebs on Security Blog, `http://krebsonsecurity.com/2011/02/spamit-glavmed-pharmacy-networks-exposed/`, February 2011.

[52] Brian Krebs. Who's behind the world's largest spam botnet? Krebs on Security Blog, `http://krebsonsecurity.com/2012/02/whos-behind-the-worlds-largest-spam-botnet/`, February 2012.

[53] Michael Levi. Social reactions to white-collar crimes and their relationship to economic crises. In Mathieu Deflem, editor, *Economic Crisis and Crime*, pages 87–105. The JAI Press/Emerald, 2011.

[54] Michael Levi and John Burrows. Measuring the impact of fraud in the UK: A conceptual and empirical journey. *British Journal of Criminology*, 48:293–318, 2008.

[55] Ariel Levite and Wyatt Hoffman. A Moment of Truth for Cyber Insurance. *Lawfare*, February 7, 2019.

[56] Kevin Liao, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin. In *Electronic Crime Research (eCrime), 2016 APWG Symposium on*, pages 1–13. IEEE, 2016.

[57] M86 Security Labs. Canadian Pharmacy no Longer King. http://www.m86security.com/labs/traceitem.asp?article=1316, May 2010.

[58] Lee Mathews. NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million. *Forbes*, Aug 16, 2017.

[59] Damon McCoy, Andreas Pitsillidis, Grant Jordan, Nicholas Waver, Christian Kreibich, Brian Krebs, Geoffrey M. Voelker, Stefan Savage, and Kirill Levchenko. PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs. In *Proceedings of the USENIX Security Symposium*, Bellevue, WA, August 2012.

[60] Microsoft Inc. Microsoft security intelligence report, volume 10, 2010. http://www.microsoft.com/security/sir/.

[61] Microsoft Inc. Microsoft security intelligence report, volume 9, 2010. http://www.microsoft.com/security/sir/.

[62] Najmeh Miramirkhani, Oleksii Starov, and Nick Nikiforakis. Dial one for scam: A large-scale analysis of technical support scams. In *14th Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, March 2017.

[63] David Modic and Ross Anderson. It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy*, 13(5):99–103, 2015.

[64] Nick Mothershaw. The 2017 Annual Fraud Report. https://www.experian.co.uk/blogs/latest-thinking/identity-and-fraud/2017-annual-fraud-indicator-results-revealed/, 2017.

[65] National Audit Office. Investigation: WannaCry cyber attack and the NHS, October 27, 2017.

[66] Terry Nelms, Roberto Perdisci, Manos Antonakakis, and Mustaque Ahamad. Towards measuring and mitigating social engineering software download attacks. In *USENIX Security Symposium*, pages 773–789. USENIX Association, 2016.

[67] NetDiligence. *Cyber Claims Study.* NetDiligence, 2015.

[68] NetDiligence. *Cyber Claims Study.* NetDiligence, 2018.

[69] Andrew Ng. How the Equifax hack happened, and what still needs to be done. *Cnet*, Sep 7 2018.

[70] Observatoire National de la Délinquance et de Responses Pénales. Victimation et Perceptions de la Sûreté, 2017.

[71] Office for National Statistics. Crime in England and Wales: year ending September 2018, 24 January 2019.

[72] Gavin O'Gorman and Geoff McDonald. Ransomware: A growing menace, 2012. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf.

[73] Jeremiah Onaolapo, Enrico Mariconti, and Gianluca Stringhini. What happens after you are pwnd: Understanding the use of leaked webmail credentials in the wild. In *Internet Measurement Conference*, pages 65–79. ACM, 2016.

[74] Letizia Paoli, Elke Van Hellemont, Cedric Verstraete, Jonas Visschers, Ralf De Wolf, Marijn Martens, Lieven De Marez, Pieter Verdegem, Evert Teerlinck, Ping Chen, Christophe Huygens, Thomas De Cnudde, Vincent Rijmen, Marie-Christine Janssens, and Thomas Marquenie. Belgian Cost of Cybercrime: Measuring cost and impact of cybercrime in Belgium. http://www.belspo.be/belspo/brain-be/projects/FinalReports/BCC_Final%20Report.pdf, 2018.

[75] Letizia Paoli, Jonas Visschers, Cedric Verstraete, and Elke van Hellemont. The Impact of Cybercrime on Belgian Business, 2018.

[76] Masarah Paquet-Clouston, Bernhard Haslhofer, and Benoit Dupont. Ransomware payments in the bitcoin ecosystem. In *Proceedings (online) of the 17th Workshop on Economics of Information Security*, Innsbruck, Austria, June 2018.

[77] Sergio Pastrana and Guillermo Suarez-Tangil. A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth. https://arxiv.org/pdf/1901.00846.pdf, 2019.

[78] Privacy Rights Clearinghouse. Chronology of data breaches, 2019. https://www.privacyrights.org/data-breaches. Last accessed February 15, 2019.

[79] Markus Riek. *Towards a Robust Quantification of the Societal Impacts of Consumer-facing Cybercrime*. PhD thesis, University of Münster, Germany, 2017.

[80] Markus Riek and Rainer Böhme. The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, 4(1), 2018.

[81] Markus Riek, Rainer Böhme, Michael Ciere, Carlos Ganan, and Michel van Eeten. Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries. In *Workshop on the Economics of Information Security (WEIS)*, University of California at Berkeley, 2016.

[82] Jeff Rumburg. Metric of the Month: Service Desk Cost per Ticket — HDI. https://www.thinkhdi.com/library/supportworld/2017/metric-of-month-service-desk-cost-per-ticket.

[83] Anton Shilov. TSMC: Outbreak of Malware That Triggered Delays & Losses Caused by Software for New Tool. *AnandTech*, Aug 9 2018.

[84] Brett Stone-Gross, Ryan Abman, Richard A. Kemmerer, Christopher Kruegel, Douglas G. Steigerwald, and Giovanni Vigna. The underground economy of fake antivirus software. In *10th Workshop on the Economics of Information Security*, Fairfax, VA, June 2011.

[85] Symantec. MessageLabs Intelligence Report, June 2010.

[86] M. Tcherni, A. Davies, G. Lopes, and A. Lizotte. The Dark Figure of Online property Crime: is Cyberspace Hiding a Crime Wave? *Justice Quarterly*, 33.5:890–911, 2016.

[87] Trend Micro. Coupon fraud could be costing your business millions. https://blog.trendmicro.com/coupon-fraud-could-be-costing-your-business-millions/, 2017.

[88] Trend Micro. Security predictions – Paradigm shifts. https://www.trendmicro.com/vinfo/ph/security/research-and-analysis/predictions/2018, December 5, 2017.

[89] UK Finance. Fraud the Facts – The Definitive Overview of Payment Industry Fraud. http://forms.cybersource.com/, 2017.

[90] UK Information Commissioner's Office. Yahoo! fined 250,000 after systemic failures put customer data at risk. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/06/yahoo-fined-250-000-after-systemic-failures-put-customer-data-at-risk/, 12 June 2018.

[91] US Attorney's Office: Eastern District of New York. Two international cybercriminal rings dismantled and eight defendants indicted for causing tens of millions of dollars in losses in digital advertising fraud, November 2018. https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing.

[92] US Department of Justice. U.S. charges Russian FSB officers and their criminal conspirators for hacking Yahoo and millions of email accounts. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions, 15 March 2017.

[93] US Postal Inspection Service. Annual report 2017. https://postalinspectors.uspis.gov/radDocs/AR2017.pdf, 2018.

[94] US Security and Exchange Commission. Altaba, formerly known as Yahoo!, charged with failing to disclose massive cybersecurity breach; agrees to pay $35 million. https://www.sec.gov/news/press-release/2018-71, 24 Apr 2018.

[95] Michel van Eeten, Hadi Asghari, Johannes M. Bauer, and Shirin Tabatabaie. *Internet Service Providers and Botnet Mitigation: A Fact-Finding Study on the Dutch Market.* The Hague: Ministry of Economic Affairs, 2011. `http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation.html`.

[96] Rolf van Wegberg, Samaneh Tajalizadehkhoob, Kyle Soska, Ugur Akyazi, Carlos Hernandez Ganan, Bram Klievink, Nicolas Christin, and Michel van Eeten. Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1009–1026, Baltimore, MD, 2018. USENIX Association.

[97] Marie Vasek and Tyler Moore. There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. In Rainer Böhme and Tatsuaki Okamoto, editors, *Financial Cryptography and Data Security*, volume 8975 of *Lecture Notes in Computer Science*, pages 44–61. Springer, January 2015.

[98] White Ops. The methbot operation, December 2016. `https://www.whiteops.com/methbot`.

[99] Gilbert Wondracek, Thorsten Holz, Christian Platzer, Engin Kirda, and Christopher Kruegel. Is the Internet for Porn? An Insight Into the Online Adult Industry. In *Proceedings (online) of the 9th Workshop on Economics of Information Security*, Cambridge, MA, June 2010. `http://weis2010.econinfosec.org/papers/session2/weis2010_wondracek.pdf`.

[100] Mingyi Zhao, Aron Laszka, and Jens Grossklags. Devising effective policies for bug-bounty platforms and security vulnerability discovery. *Journal of Information Policy*, 7(372–418), 2017.