DEMOS

THE GREAT CYBER SURRENDER

HOW POLICE AND GOVERNMENTS ABANDON CYBERCRIME VICTIMS

ASLI ATAY
JAMES SWEETLAND
HARRY CARR

NOVEMBER 2020

Clario Tech Limited is a London-based cybersecurity company. It was founded in 2019 to disrupt the security software industry by securing people's digital lives with a human, customer-focussed approach to cybersecurity and act as a consumer champion. Clario employs more than 800 people including a large number of Apple Certified Tech experts and launched its new product in Q2 2020.

Published by Demos November 2020

15 Whitehall, London, SW1A 2DD
T: 020 3878 3955
hello@demos.co.uk
www.demos.co.uk

FOREWORD

I am proud to present *The Great Cyber Surrender: How Police and Governments Abandon Cybercrime Victims*, the first transatlantic research study of its kind investigating the issue of cybercrime and its impact on consumers in the United Kingdom and the United States of America.

I want to personally thank all participants of this report, especially those victims who were kind enough to share their experiences with us; and, of course, those cybersecurity experts who graciously shared their knowledge with us. Without the contribution of these individuals, this report would not exist.

I've spent the last two years with my team building Clario, a new cybersecurity product which makes digital security easy for all with in-built education, 24/7 human support and a user-friendly approach. We were well aware of the escalating cybercrime crisis, but even we were surprised how ill-equipped our society is in trying to keep up with an opponent that is constantly evolving.

As this report reveals, many people feel unsupported, don't know where to turn when they fall victim, and the long-term emotional impact that victims feel can be huge. Significant changes in legislation, corporate cultures, education and personal consciousness are needed to fight the growing threat of cybercrime.

The best line of defence is a public equipped with the tools and knowledge to protect themselves, but even our greatest efforts will only ever be a drop in the ocean if governments don't accelerate their approach. We hope that this report drives action on both sides of the Atlantic.

Scarlet Jeffers
VP of Experience
Clario Tech

November 2020

CONTENTS

ACKNOWLEDGEMENTS **PAGE 5**

EXECUTIVE SUMMARY **PAGE 6**

METHODOLOGY **PAGE 9**

INTRODUCTION **PAGE 10**

CHAPTER 1 **PAGE 11**
NATURE AND SCALE OF CYBERCRIME IN THE US & UK

CHAPTER 2 **PAGE 18**
THE IMPACT ON VICTIMS

CHAPTER 3 **PAGE 24**
THE CURRENT SYSTEM - AND WHY IT IS NOT FIT FOR PURPOSE

CHAPTER 4 **PAGE 34**
HOW TO FIX IT

GLOSSARY **PAGE 38**

ACKNOWLEDGEMENTS

First and foremost, we would like to thank the interviewees who took the time to speak with us for this report. This included over 20 victims of cybercrime, who bravely shared their stories and experiences with us - their contributions helped keep us focused on the human cost of these crimes. Thanks must also go to our 11 expert interviewees from the US and UK, who generously shared their perspectives on the problem of cybercrime, despite the travails of transatlantic Zoom connections. We owe particular gratitude to Mark Montgomery, Rob Morgus, Joel Lewis and Rick Muir, for agreeing to share additional comments on our policy recommendations, following their first interviews.

Thanks must also go to all our colleagues at Demos - many of whom contributed suggestions and ideas which helped shape our report into the final document presented here. More specifically, our thanks to Alex Krasodomski-Jones for his insight on policy recommendations, Maeve Thompson and Josh Tapper for their guidance on communication, and Maiyoraa Jeyabraba for proofreading the report. In addition, we thank Claudia Wood for her work producing the evidence review, which provided a vital foundation for our own research and analysis.

Finally, we would like to thank everyone at Clario for making this project possible, as well as our partners at MSL, who were a guiding hand in putting together this report. In particular, Frank Bruce and Abigail Smith at MSL, for their involvement and hard work throughout this extensive project.

All errors and omissions are entirely our own.

Asli Atay
James Sweetland
Harry Carr

November 2020

EXECUTIVE SUMMARY

One thing is certain: we are under attack.

As our reliance on the internet to work, shop, bank and socialise increases, networks of international cybercriminals lie in wait to exploit any and every opportunity to steal, scam and deceive. Those of us yet to fall victim take comfort in the idea that our governments and law enforcers are equally tireless in responding to this threat. Those less fortunate have found the opposite to be true.

In this, the most comprehensive transatlantic study of its kind, we find that the approach of both police and policymakers to tackling cybercrime is so inadequate that it is tantamount to surrender. On both sides of the Atlantic, we find no systematic attempt to combat cyber fraud at scale. We find millions of victims left to deal with feelings of powerlessness, violation and shame alone. We find the quest for justice largely abandoned by forces without the skills or networks to hunt down perpetrators. In the battle to keep our online spaces safe from cybercrime, we are not just losing. We have lost.

And at such cost. According to Cybersecurity Ventures, economic losses due to cybercrime are estimated to exceed the total GDP of all countries but the US and China by 2021, and the total cost will amount to around six trillion dollars by 2021.[1] One in three Americans and one in five Britons has been a victim of cybercrime - equivalent to 126 million people across the two countries, many suffering from serious psychological effects alongside financial losses. Chronic underreporting across the spectrum of online crime suggests that these figures are just the tip of the iceberg.

This report, made possible by Clario, is an urgent call to arms. We call for an immediate and comprehensive overhaul of national and international responses to this complex, enormous and evolving threat. We call for more support for victims and greater resources for law enforcement to develop the technical skills needed to fight cybercrime on the front line. We call for an end to public acceptance that use of the internet will always carry an element of criminal risk, and a renewed commitment from our leaders to fight for our future online safety, as an international priority - for us, and for the generations to come.

KEY FINDINGS

1. **One in three Americans and one in five Britons have been victims of cybercrime.** Some 35% of Americans and 21% of Britons say they have had their data accessed illegally. This equates to 115 million people in the US and 11 million people in the UK. More than one in ten Britons (11%) and nearly one in five Americans (19%) say they have had their data accessed illegally in the last 12 months.

2. **Understanding the true scale of the problem is particularly difficult, due to underreporting**. Victims are often unsure how to report, or doubt anything will be done, so numbers are undoubtedly higher than the tally reported to law enforcement agencies. Our poll findings suggest that only one in four Britons (27%) and four in ten Americans (40%) who were victimised online reported the crime to the government or the police. One in three Britons (33%) and Americans (34%) aren't confident that they would know what to do if they became a victim of online fraud.

3. **Law enforcement and victim support regarding cybercrime are woefully inadequate in both the UK and the US**.

   The methods by which cybercrime is reported to and managed by law enforcement are fundamentally distrusted by victims, law enforcement and experts. Action Fraud in the UK in particular is not fit for purpose.

1. Morgan, S. Cybercrime to Cost the World $10.5 Trillion Annually by 2025. Cybersecurity Ventures, 2020. Available at: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ [Accessed 27/11/2020]

Top-level law enforcement does have some capability to tackle complex cybercrime, but lacks the capacity (or resources) to do so at scale. By contrast, local police lack both the capability and the capacity to deal with these crimes. They do not have anything like the required skillset to combat cybercrime, in the current system. Despite this, all but the most serious cybercrime cases are left for local law enforcement to be handled - if such investigations are even pursued at all.

Law enforcement is not doing enough to support the victims of cybercrime in both countries. Law enforcement in both countries do not possess the skills to deal with cybercrime and fail to support the victims of these crimes emotionally.

4. **Many victims suffer serious psychological effects alongside the financial cost of cybercrime**. People report feeling powerless or stigmatised after these events. Romance scams inflict particular devastation and shame upon their victims. In some cases, victims suffer even more severe psychological impacts - including self-harm, suicidal thoughts and depression.

5. **People are aware that there are dangers in principle, but are not protecting themselves in practice.** The majority of Americans and Britons alike are worried about their data being accessed illegally (64% of Americans, 58% of Britons), but are not investing in protecting themselves from hackers (55% of Americans and 59% of Britons do not invest in protecting themselves from online fraud).

   This appears to be due to a combination of complacency, fatalism, and a lack of know-how. One in three Britons (26%) and Americans (26%) say they could find out how to protect themselves online, but have chosen not to do so. A further one in ten (9% of Britons, 9% of Americans) think it is impossible to understand how to stay safe online. And one in four Britons (27%) and Americans (25%) think there is nothing that can be done if a hacker decides to access their data, no matter the security measures they put in place.

6. **Cybercriminals are agile and innovative, leaving law enforcement struggling to keep up**. Criminal tools, such as malware or ransomware, are bought, sold and shared quickly in online marketplaces, via the 'cybercrime-as-a-service model'. This means that even the least tech-savvy criminals can access and deploy malicious software, to defraud or target everyday consumers. In addition, the COVID-19 pandemic has led to a suite of criminal developments, whereby existing scams are repackaged to target pressing fears or anxieties - e.g. masks scams or phishing related to personal protective equipment.

Informed by these findings, *The Great Cyber Surrender* makes ten recommendations to fix the currently broken system, seeking to prevent and tackle cybercrime, and deal with its repercussions. This report focuses on the US and UK, both of which have vital opportunities to change course on cyber policy - the former faces the start of a new presidential term, the latter will replace its National Cyber Security Strategy after 2021. But these policies deserve consideration from governments across the world, in trying to tackle the international threat posed by cybercrime.

THE GREAT CYBER SURRENDER RECOMMENDS THAT BOTH THE US AND UK GOVERNMENTS:

1. Establish and promote a National Reporting Hotline for fraud and cybercrime, with a simple three-digit number, e.g. '119 for Cybercrime.'

2. Establish a National Fraud Taskforce, staffed with specialist investigators, with responsibility for investigating cybercrime cases.

3. Roll out Victim Care Squads nationally, staffed with specialist advocates, to provide support and advice to victims of cybercrime.

4. Legally oblige banks to pass anonymised information to the new National Reporting Hotline, whenever their customers are victimised by cybercrime.

5. Establish a legal duty that, whenever a data breach occurs, businesses must provide customers with timely, step-by-step guidance on how to protect themselves and must also introduce remedial security measures - such as mandatory multi-factor authentication on customer accounts.

6. Mandate basic cybersecurity education within schools (particularly in the US, where provision is far more uneven) to increase digital literacy, awareness and knowledge of protection.

7. Introduce a national campaign to educate adults on cybersecurity, based around the launch of the new National Reporting Hotline.

THE GREAT CYBER SURRENDER RECOMMENDS THAT THE US GOVERNMENT:

8. Strengthen the Cyber Infrastructure Security Agency (CISA), providing it with sufficient resources to coordinate private-public collaboration for combating cyber threats.

9. Introduce a post of National Cyber Director, responsible for enhancing the US' public-private work and international collaboration efforts.

THE GREAT CYBER SURRENDER RECOMMENDS THAT THE UK GOVERNMENT:

10. Reach effective security and policing agreements with the EU, following Brexit, to ensure British police forces retain access to European intelligence and joint investigative work.

METHODOLOGY

Methodologically, our research builds upon four main pillars:

- A comprehensive evidence review, looking at academic and grey literature to explore what others see as the key problems in this field.
- Two nationally representative polls of 2,000 people each from the US and UK, to understand public experiences, behaviours and attitudes regarding cybersecurity and cybercrime.
- Twenty case studies of victims of cybercrime, drawn from a diverse set of demographic backgrounds across the UK and US, who shared their personal stories of how they became victims and the emotional impact of their experiences.

Finally, we spoke with eleven experts, encompassing a wealth of knowledge and experience from law enforcement, academia, NGOs, the private sector and government. We are grateful for their time and contributions, which helped shape the policy recommendations produced by this research report. These experts are:

- **Dr Ingolf Becker** - Lecturer in the Department of Security and Crime Science at University College London (UCL), where he works on information management and cybersecurity.
- **Sherrod DeGrippo** - Senior Director of Threat Research and Detection for ProofPoint, a cybersecurity firm which works with businesses to protect them from cyberthreats.
- **Kristin Judge** - CEO of the Cybercrime Support Network, a US-based nonprofit which supports cybercrime victims by improving collaboration between national partners. She serves on the Board of Advisors for Cybersecurity Ventures.
- **Professor Michael Levi** - Professor in the School of Social Sciences at Cardiff University, an internationally-renowned expert in cybercrime and organised crime, with experience advising Europol, the Home Office, and the United Nations.
- **Joel Lewis** - Consumer and Financial Service Policy Manager for Age UK, a charity which provides advice and support to older and vulnerable people, in the UK.
- **Mark Montgomery** - Executive Director of the Cyberspace Solarium Commission, a body tasked with developing a new strategy to protect the US from cyberattacks. He serves on the Board of Advisors for Cybersecurity Ventures.
- **Rob Morgus** - Senior Director of the Cyberspace Solarium Commission.
- **Rick Muir** - Director of the Police Foundation, the UK's leading independent policing think-tank.
- **Chris Painter** - President of the Global Forum on Cyber Expertise Foundation Board, formerly a prosecutor, chair of the G8's High Tech Crime Group, and the world's first cyber diplomat at the US State Department.
- **Alex Rothwell** - Deputy National Coordinator of Fraud and Economic Crime at the City of London Police, the British police force responsible for leading on economic crime.
- **Wayne Stevens** - Fraud Lead for Victim Support, a UK-based organisation which provides emotional support and advice to people who experience any form of crime.

INTRODUCTION

The world in which we live is increasingly dominated by our use of digital devices. From smartphones to laptops, to the Internet of Things, technology's impact on our everyday lives has become ever more pronounced. In the age of COVID-19, this dependence is even greater, as these digital technologies have become vital to our ability to work, communicate and connect with one another.

And yet, the use of these devices exposes us to new forms of malicious activity. Cybercrime and cyber fraud are now established as highly effective means for criminals to generate large sums of money. In this report, we are concerned with two types of cybercrime. First, **cyber-dependent crimes**, which are those that could only be committed using a computer, digital tool or network, such as hacking into a computer. Secondly, there are **cyber-enabled crimes**, which can occur without computers, but are aided by the use of digital tools. An example of this would be fraud: while it increasingly occurs digitally, including via scam emails, fraud can happen offline and is therefore not dependent on cyber tools.

When we think about cybercrime, we tend to focus solely on its financial and technical components: the hacking of an account, the loss of data, and the transferring of money to unknown third-parties. While these are central to what we mean by cybercrime, this approach overlooks the human costs of these offences. We forget the emotional impact of discovering that someone has been able to access your private data. We ignore the stigma attached to reporting this crime, whether this means sharing your experience with family, friends or through official channels. We fail to acknowledge that there are deep psychological harms associated with being the victim of these increasingly common forms of crime.

The Great Cyber Surrender seeks to confront this failure. We want to change the narrative around the cost of cybercrime by exploring the emotional impact on victims, identifying why we are failing to tackle these offences, and demonstrating how we can build a new strategy to stop consumers suffering these crimes. Our research shows that cyber policy and digital policing is woefully inadequate in the US and UK, as things stand.[2] In this report, we will highlight these issues, explore the costs they impose on victims and identify what we can do to fix them.

Overall, our research shows that the current approach to tackling cybercrime in the US and UK is failing in various ways. **Chapter 1** discusses the nature and scale of the cybercrime problem in more detail, looking at both the UK and US. This chapter emphasises what makes someone vulnerable to cybercrime and explains why there is such a crisis of underreporting with digital crimes.

Chapter 2 examines the deeper effects of cybercrime, looking closely at the emotional and mental health consequences of these incidents upon their often vulnerable victims. We look at the shame, stigma and powerlessness felt by people who suffer these crimes, to explore the impacts of cybercrime, beyond the simple financial losses involved.

Following this, in **Chapter 3**, we look at the current policy landscape and law enforcement response in the US and UK, to demonstrate exactly how it is unfit for purpose. This chapter identifies a clear cyber skills gap, where law enforcement is constantly outmatched by agile and innovative cybercriminals. In addition, we evaluate two other issues: (1) the effect of COVID-19 upon cybercrime and (2) the threat posed by Brexit to the UK's cyber policing.

The Great Cyber Surrender concludes with solutions to the problem. In **Chapter 4**, we propose ten policy recommendations to help confront cybercrime in both the US and UK. In doing so, we seek to construct a new, more caring, victim-centred approach to dealing with cybercrime, which protects consumers from unnecessary harm and recognises the emotional costs of this crime.

2. In the UK, central bodies like the National Crime Agency provide services across the entire country. By contrast, policing in the UK is devolved, meaning that Scottish policing is run by the Scottish Government, while policing in England and Wales is run by the British government. For consistency, we refer to the 'US' and 'UK' throughout this report, for ease of comparison, but readers should note that any reference to 'UK policing' found here alludes to English and Welsh policing alone.

CHAPTER 1
NATURE AND SCALE OF CYBERCRIME IN THE US AND UK

KEY FINDINGS

- Some 35% of Americans and 21% of Britons say they have had their data accessed illegally - this equates to 115 million people in the US and 11 million people in the UK.
- Only one in four Britons (27%) and four in ten Americans (40%) who were victims reported the crime.
- One third of Britons (33%) and Americans (34%) do not know what to do if they become a victim of cybercrime.
- People are fatalistic about cybercrime. One in four Britons (27%) and Americans (25%) think there is nothing that can be done if a hacker decides to access their data, no matter the security measures they put in place.

Cyber criminals are building their own niche economies and developing innovative methods as more people use online spaces. They are agile in coming up with new methods and adaptive to changes in technology. Rob Morgus, Senior Director at the U.S. Cyberspace Solarium Commission, stated that a study by Accenture estimates in the five years to 2024, approximately, $5.2 trillion could be lost to cybercrime. This figure is global but a substantial amount of that will likely be in the United States.[3]

In this chapter, we discuss the nature and scale of cybercrime in the US and the UK. Then we explore who is more likely to be a victim of cybercrime and what the problem of underreporting means if we have to develop policies to fight with cybercrime effectively.

1.1 CYBERCRIME IN THE US

We conducted two nationally representative polls to understand people's attitudes towards cybercrime in the UK and the US. **We found that more than one third of Americans have had their data accessed illegally (35%). That is more than 115 million people**. Twenty percent of victims lost something personal or of sentimental value that couldn't be recovered (23 million people) and 11% lost money as a result (13 million people).

Among those who lost money when their data was compromised, the mean amount lost was $1,231.

3. Abbosh, O. and Bissel, K. Securing the Digital Economy: Reinventing the Internet for Trust. Accenture, 2020. Available at: https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50 [Accessed 14/10/2010]

In 2014 according to the US Department of Justice, only 7% of Americans were the victim of identity theft.[4] In 2018, according to the annual crime survey one in four Americans were victims of cybercrime. This study was based on a narrow definition of cybercrime, excluding types of cybercrime other than cyber-enabled fraud.[5]

The Internet Crime Complaint Center (IC3) of the FBI stated that in 2019 it received the highest number of complaints and the highest dollar losses reported since its establishment in 2000. In 2019, it received 467,361 complaints, an average of nearly 1,300 every day,[6] with $3.5 billion being lost – a figure that has tripled in 5 years.[7]

While this dollar loss figure combines the losses of all complainants (businesses and individuals), the single biggest category for dollar loss is where businesses are targeted, in the form of Business Email Compromise (BEC),[8] which saw US businesses lose $1.7 billion last year. The second biggest dollar loss came from romance fraud. According to the FBI's report, nearly 20,000 Americans were victims of romance fraud and $475 million was lost as a result of it.[9] The most commonly reported cybercrime, however, was phishing – with 114,000 victims losing $500 each on average.[10]

While the numbers clearly show the rise in cybercrime, it's highly likely these don't tell the full story due to underreporting. **We found that 60% of Americans who were victims of cybercrime did not report the crime to the government.**

1.2. CYBERCRIME IN THE UK

Our research found that one in five Britons have had their data accessed illegally (21%), equivalent to 11 million people. Almost one in every six victims lost money as a result (two million people) and almost one in every eight victims lost something personal or of sentimental value that couldn't be recovered (1.6 million people). Among those who lost money, the mean amount lost was £1276 in the UK.

According to the National Fraud Intelligence Bureau (NFIB), which records cybercrime across the UK, between July 2019 and July 2020, there had been 32,518 reports of cyber-enabled crime in the UK. 89% of these came from individual consumers, totalling more than £2 million, while 11% came from organisations, reporting losses of £5.7 million.[11] According to the NFIB from July 2019 to July 2020 period, 50% of all cyber dependent crimes reported were hacking social media and email, 24% virus or malware, 15% hacking personal, 11% hacking extortion and 1% hacking server.[12]

However, these numbers are expected to be an underestimate due to the low number of reporting of cybercrime. **We found that seven in every ten victims (70%) didn't report it.**

The NFIB records cyber-dependent crimes under fraud statistics. In the same July 2019 to July 2020 period, there were 392,762 reports of fraud, with losses amounting to £2.7 billion. More than two thirds (69%) of these were defined as cyber-enabled, with £204m lost by businesses and £1.6bn lost by individuals.[13]

1.3. ANYONE CAN BE A VICTIM

In general, the research on the victims of cybercrime in the UK or the US is quite limited. A survey was conducted with over 11,000 people to examine whether certain personalities or socio-demographic characteristics made people more prone to being a victim of cybercrime. The research found that men in their 20s and 30s are most vulnerable to cybercrime simply due to the fact they are peak users, while it is generally also believed that older people are more vulnerable to cybercrime.[14]

In 2019, a study from the Cyber Security Centre at the University of Warwick[15] attempted to predict susceptibility to "cyber-fraud victimhood", looking at personality traits and demographic factors which made people susceptible to online frauds and scams, including romance scams. They found that younger people were more likely to engage in

4. B. Lynn Winmill, David L. Metcalf and Michael E. Band. Cybercrime: Issues and Challenges in the United States. Digital Evidence and Electronic Signature Law Review, Vol 7. 2010. Available at: https://sas-space.sas.ac.uk/5511/1/1921-2705-1-SM.pdf [accessed: 12/10/2020)
5. Clement, J.L. U.S. consumers and cyber crime - Statistics & Facts. 2019. Available at: https://www.statista.com/topics/2588/us-consumers-and-cyber-crime/ [accessed: 12/10/2020]
6. FBI Internet Complaint Centre. 2019 Internet Crime Report. 2019. Available at: https://pdf.ic3.gov/2019_IC3Report.pdf. [accessed: 12/10/2020]
7. Statista. Complaints about Internet crime on the IC3 website from 2000 to 2019. 2019. Available at. https://www.statista.com/statistics/267546/number-of-complaints-about-us-internet-crime/ [accessed: 12/10/2020]
8. BEC is a scam where legitimate business email accounts are compromised to conduct unauthorized transfers of funds.
9. FBI Internet Complaint Centre. 2019 Internet Crime Report. 2019. Available at: https://pdf.ic3.gov/2019_IC3Report.pdf. [accessed: 12/10/2020]
10. Ibid.
11. NFIB Fraud and Cyber Crime Dashboard - 13 months of data. 2019. Available at: https://colpolice.maps.arcgis.com/apps/opsdashboard/index.html#/60499304565045b0bce05d2ca7e1e56c [accessed 10/10/2020]
12. Ibid.
13. Ibid.
14. Narisi. S. Who's the most likely cyber-crime victim?. 2011. Available at: http://www.itmanagerdaily.com/most-likely-cyber-crime-victim/ [accessed 10/10/2020]
15. Whitty, M. Predicting susceptibility to cyber-fraud victimhood. 2019. Journal of Financial Crime. Available at: https://www.emerald.com/insight/content/doi/10.1108/JFC-10-2017-0095/full/html#sec010 [accessed 10/10/2020]

routine activities that potentially expose them to cyber-frauds, while older people were more likely to engage in "online guardianship" behaviours.

The research concluded that age, some personality traits that are defined by the search for experiences and by the readiness to take physical, social and financial risks for the sake of such experiences made certain people much more likely to become victims. Researchers were surprised that education tended to increase the chances of being vulnerable to cybercrime, and suggested that this could be down to complacency: "educated people might be more likely to hold the view that they can spot a scam, and thereby spend less efforts seeking out persuasion and deception cues."[16]

Our research found that there is no conclusive evidence to say certain demographic groups are more likely to be a victim. Spending more time online or certain psychological traits might increase people's likelihood of being a victim. **But in fact, our research shows that all walks of life can be victimised.**

1.3.1. Complacency and fatalism

Our polling findings show that complacency is a serious issue when it comes to public attitudes to cybercrime: most people are aware of the dangers in the theory, but many are not taking practical precautions in line with this knowledge.

Four in ten Britons (43%) and Americans (39%) think they are vulnerable enough to be targeted by hackers.

Although many people feel vulnerable to cybercrime, less than half of the population in both countries invest in digital tools to help protect themselves from online fraud. 59% of Britons and 55% of Americans do not spend any money to protect themselves from online fraud.

One in four Britons (27%) and Americans (25%) think if a hacker decides to hack their data they will be able to do it no matter what security measures are in place.

Which of the following comes closest to your views?

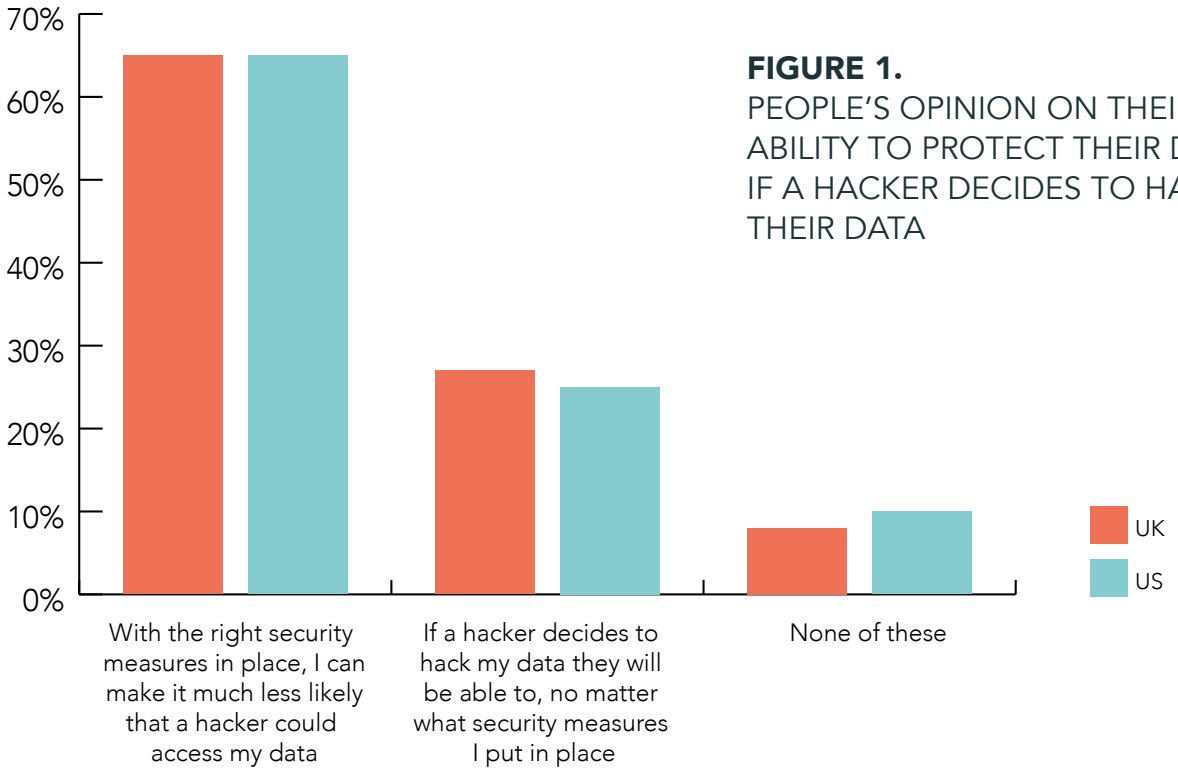


FIGURE 1.
PEOPLE'S OPINION ON THEIR ABILITY TO PROTECT THEIR DATA IF A HACKER DECIDES TO HACK THEIR DATA

16. Whitty, M. Predicting susceptibility to cyber-fraud victimhood. 2019. Journal of Financial Crime. Available at: https://www.emerald.com/insight/content/doi/10.1108/JFC-10-2017-0095/full/html#sec010 [accessed 10/10/2020]

Britons worry about having their data stolen, but are ominously more relaxed about the common methods by which it happens. More than half of Britons (58%) said they're worried about their data being accessed illegally, but 50% of them say they are not worried about being a victim of phishing and the majority don't think they're vulnerable to ransomware (56%).

More than two thirds of Americans (64%) are worried about their financial information being accessed illegally, but similar to Britons, almost half of Americans said they are not worried about being a victim of a phishing scam (47%) or ransomware (48%).

This is despite ransomware being a particularly significant threat, both to individuals and businesses, within the modern cybercrime landscape.[17] Several of our experts highlighted the prevalence and increasing popularity of this kind of crime:

> *"The last big change is ransomware, and I think that was the innovation that really was massive… Because suddenly you can lock people out of their personal data and they will often have a strong incentive to pay the criminals."*
> Dr Ingolf Becker, UCL

> *"I think the move to more strategic ransomware operations is very scary."*
> Sherrod DeGrippo, Senior Director of ProofPoint

Which of the following comes closest to your views?

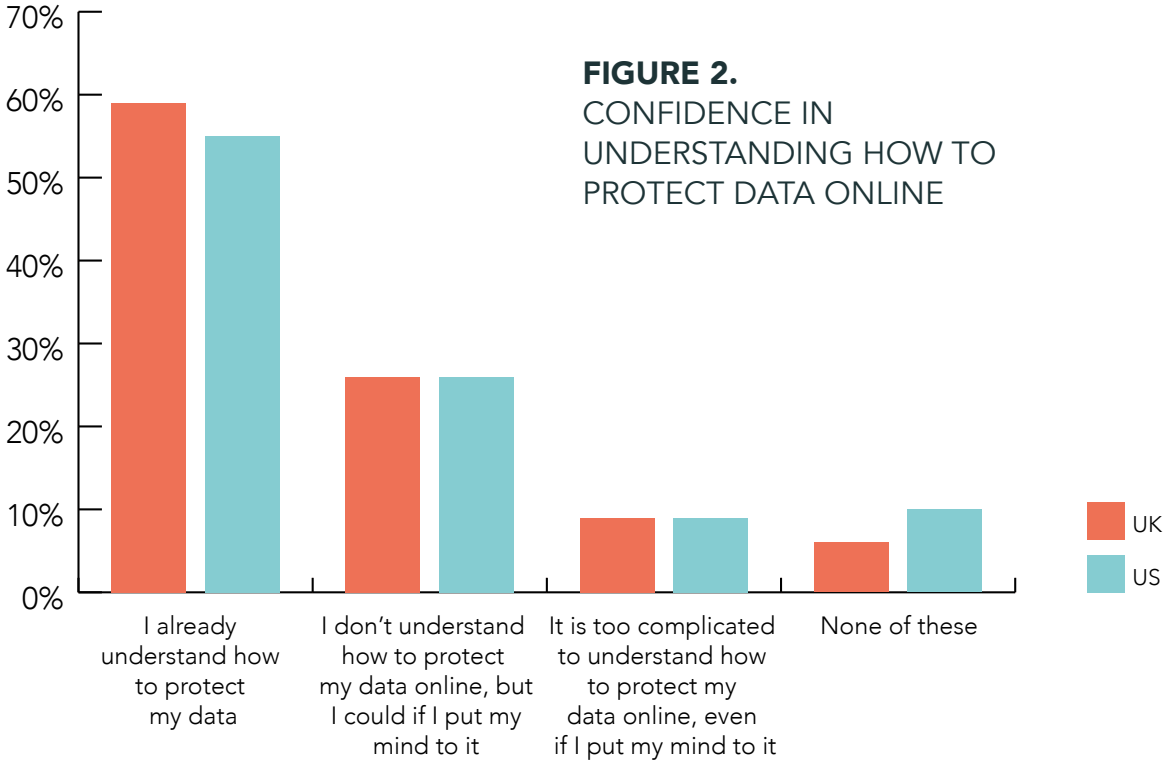


FIGURE 2.
CONFIDENCE IN UNDERSTANDING HOW TO PROTECT DATA ONLINE

17. Ransomware is a specific form of malware which locks a device and (usually) encrypts the data held on it. A ransom is then demanded from the user, to restore access to their data or device. This kind of malware is targeted at both individuals and larger organisations

People think they know how to protect themselves but as revealed by the huge number of victims in both countries, that is far from the truth. Actually, many admit they don't know how to protect themselves. Looking at the polling data, we see that more than one in three Britons don't know how to protect their data online (35%); one in ten (9%) think it's impossible for them to understand, while a quarter (26%) say they can't be bothered to find out how to do so. Similarly, one in four Americans (26%) think they don't know how to protect their data online but they could do it if they put their mind to it whereas 9% think it's impossible for them to understand.

Men were more confident than women in both countries. For instance, 65% of men in the UK said they already understand how to protect their data online, compared with 53% of women who said the same. On the other hand, as we discussed in more detail in Section 1.3, middle aged men are more likely to be victims of cybercrime.

Many people are also fatalistic about cybercrime. More than a quarter of Britons (27%) and 25% of Americans think there is nothing that can be done if a hacker decides to access their data, no matter the security measures they put in place.

Thinking about the security of your personal and financial information online, how much, if at all, do you believe the government is able to do to protect people from online fraud?

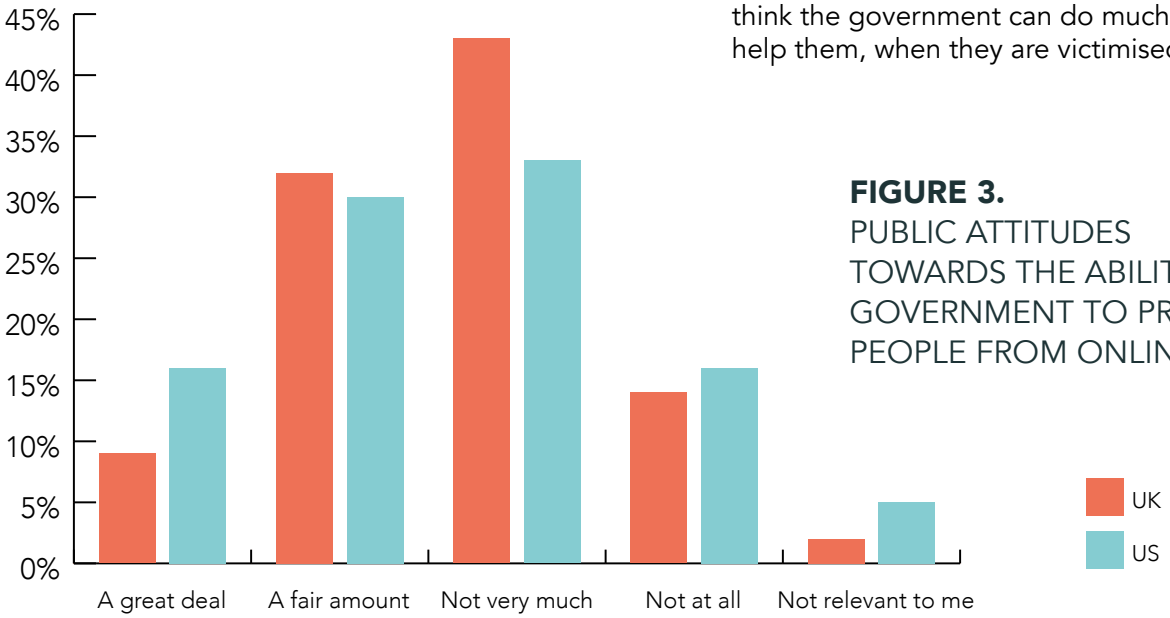


FIGURE 3.
PUBLIC ATTITUDES TOWARDS THE ABILITY OF GOVERNMENT TO PROTECT PEOPLE FROM ONLINE FRAUD

1.4. UNDERREPORTING IS A MAJOR PROBLEM IN POLICYMAKING

The awareness of cybercrime and the amount of research on cybercrime has grown rapidly over the last few decades, but underreporting remains a massive issue.

The Great Cyber Surrender findings suggest that only a quarter of victims reported the crime (27%) in the UK. This is also consistent with Britons' experience of reporting cybercrime. Among the 27% who reported cybercrime, the majority of the Britons (57%) didn't find the services helpful. More than one third of Britons reported that the law enforcement tried to help, but they couldn't do much and 19% said they did nothing at all.

Six out of every ten Americans (60%) who were victims of cybercrime did not report the crime to the government. Of those that did, more than one third (37%) didn't find it helpful. Almost one in three Americans (30%) who reported crime said the law enforcement tried to help them but couldn't do much. Seven percent said the law enforcement did nothing at all.

In the UK, there is strong dissatisfaction with the approach of the government and the legal system to cybercrime - three in five think they are not doing enough to protect people from online fraud. 59% of Britons think the government is not doing enough to protect the people whereas 63% thinks the legal system is not doing enough.

More than half of Americans (55%) think the legal system is not doing enough to protect people from online fraud. In addition, 49% of Americans don't think the government can do much or anything to help them, when they are victimised.

Lack of reliable data on cybercrime makes it difficult to assess what cybercrime really costs. And without reliable data, law enforcement can't fight against cybercrime effectively.

There are many reasons why cybercrime is underreported. Victims often lack full information on how to respond or what actually happened.

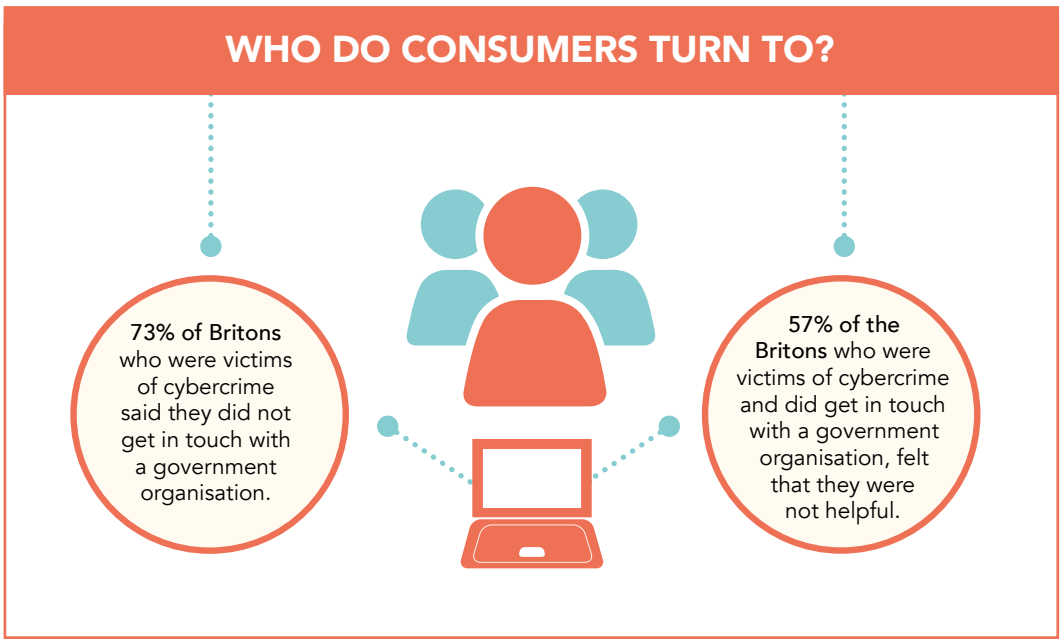
> *"In terms of reporting, if you ask someone in the street if they know what to do when they have been a victim of cybercrime they have no idea who to contact."*
> Ingolf Becker, Lecturer at Department of Security and Crime Science at UCL

In many cases, victims might not know where to report or believe that law enforcement has the capability to do anything.[18]

The situation is slightly different for banks and businesses. Companies spend huge amounts of money on cybersecurity. Mark Montgomery, the Executive Director of the Cyberspace Solarium Commission, states that banks and businesses spend on average 3% to 4% of their IT budget on cybersecurity. However, he argues that they need to double what they spend right now and should be spending 10 to 12% of their IT budget on security - which would mean many millions of dollars.[19]

Some factors can disincentivise companies to report cyber incidents. Reputational costs are high; companies do not want to look incompetent at holding their customers' data. In addition to reputational costs, companies can face civil and criminal penalties, which might disincentivise them from reporting cybercrime, particularly if reporting reveals data mishandling. For example, the Information Commissioner's Office announced its intention to fine British Airways over £180m in July 2019, after it reported loss of data related to a fraud incident.[20] While BA appears unlikely to pay this substantial sum, it highlights part of the reason companies may be reticent to report cybersecurity breaches.[21]

Moreover, sometimes companies want to keep cyberattacks secret to prevent further attacks. A cyber incident might make the company look weak. When Sony was hacked in 2011, 20 other smaller cyberattacks followed.[22] Like they say, blood in the water might attract other sharks.



18. McGuire, M and Dowling, S. 2013. Cyber crime: A review of the evidence Research Report 75 Summary of key findings and implications. Home Office. Available at: Science) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf [accessed 12/10/2020)
19. Interview, Mark Montgomery and Rob Morgus.
20. Information Commissioner's Office. Intention to fine British Airways £183.39m under GDPR for data breach. 2019. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ [accessed 12/10/2020]
21. Lawyer Monthly. BA Expects to pay only £20 million of £183 million fine. Lawyer Monthly. August 2020. Available at: https://www.lawyer-monthly.com/2020/08/ba-expects-to-pay-only-20-million-of-183-million-fine/ [accessed 12/10/2020]
22. Richmond, R. 2013. What's in a number? Estimating the cost of cybercrime. Online. Available at: https://eiuperspectives.economist.com/technology-innovation/measuring-cost-cybercrime/article/what%E2%80%99s-number-estimating-cost-cybercrime [accessed 12/10/2020]

CASE STUDY – TRACY

Tracy is a woman in her 50s and lives in New York. She has a bachelor's degree from a college in Boston. She has worked for several high profile media companies in Manhattan.

Tracy is digitally competent. She describes herself as glued to her phone and does everything online. She doesn't even remember the last time she actually went to a store.

One day she received a call telling her another purchase was made on her account.

"I had to fight tooth and nail to get money refunded and had to go through all sorts of machinations to prove I didn't make the purchase."

Thousands of dollars were taken from her account. She didn't go to the police, instead trying to deal with the issue with her bank. The process took weeks - she had to spend hours on calls and eventually involve her lawyer.

Being hacked had a serious detrimental effect on Tracy's mental and physical health. She increased her dose of antidepressants; she ate unhealthily due to stress, putting on 20 lbs in weight, and she began to use alcohol as a crutch.

"Quite frankly, you know, that one glass of wine at night ended up being three glasses of wine a night. I would eat the wrong things because I'd be so stressed, I just needed something to enable me to relax and stop thinking. So, that was bad, 20 lbs added, was not a good thing."

The experience has left Tracy with serious issues around trust which have affected her daily life. She no longer shops or does online banking using her phone, and the impact has affected her personal relationships:

"It has gotten to the point where I don't trust anybody. If someone came up and said to me, 'The sky is blue', I would probably do a double check."

CHAPTER 2
THE IMPACT ON VICTIMS

KEY FINDINGS

- Many victims suffer serious psychological effects alongside the financial cost of cybercrime.
- Romance scams inflict particular devastation and shame upon their victims.
- In some cases, victims suffer even more severe psychological impacts - including self-harm, suicidal thoughts and depression.
- Among victims who note a psychological impact, 75% experience stress, 70% anxiety, 52% fear, 51% shame, 48% anger and 43% isolation.
- Many people trust banks or tech companies to deal with cybercrime, but don't feel comfortable during the process because the response of companies vary to a great extent.

Sometimes referred to as a victimless crime, we often overlook the emotional cost of being a victim of cybercrime. Being a victim of cybercrime is more than losing your personal or financial information online.

> *"**Being a fraud victim can leave people highly disturbed, distressed, feeling vulnerable and insecure**; those impacts play out in so many different ways and it'll depend on personal and historic experiences. Significant fraud victimisation can sometimes raise previous trauma for you and so counselling or therapeutic services might be one way of tackling that."*
> Wayne Stevens, Fraud Lead, Victim Support

Unfortunately, only few places acknowledge the emotional impact of going through the experience of cyber crime in their services. In order to better understand the individual experiences, we interviewed twenty victims of cybercrime from the UK and the US.

Victims of cybercrime often experience a turmoil of emotions. The shock of realising what had happened, the anger and blame are common emotions many victims experience. Often embarrassment and shame are associated with being a victim of cybercrime. In some occasions, the emotional impact has long-term consequences and even leads to a withdrawal from online spaces and wider trust issues.

2.1 EMOTIONAL DISRUPTION

When we asked how being a victim of cybercrime made them feel, many interviewees said they felt worried, anxious and angry. They often

blamed themselves for falling for a scam, worried about taking their money back and losing more information to another cyber attack.

Many of them were shocked because they didn't know why they became victims of cybercrime in the first place. Some businesses already have good measures in place. They trace suspicious activities and notify their customers immediately. However, receiving that letter or email stating that their data was compromised can cause great anxiety and confusion.

This is quite consistent with previous research. Research conducted in 2010 with 10,000 people in 10 countries showed that the majority of victims feel angry (58%) and annoyed (51%). 40% of victims feel cheated and they blame themselves for being attacked.[23]

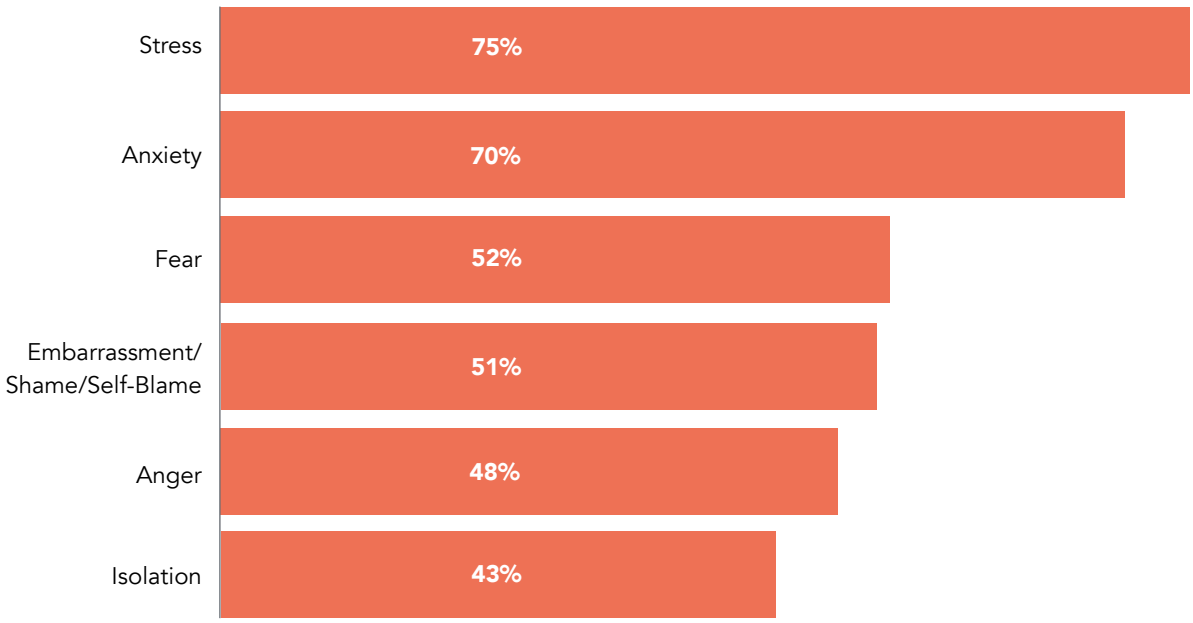
Similarly, a study conducted by the University of Portsmouth in April 2020 noted psychological impacts such as anger, anxiety, fear, isolation and embarrassment.[24] The study found that among those victims noting any impact (great or fair amount): 75% noted stress, 70% anxiety, 52% fear, 51% embarrassment/shame/self-blame, 48% anger and 43% isolation.

One of the reasons for going through lots of negative emotions is not knowing what to expect from the process. Even though many people trust banks or tech companies to deal with cybercrime, they still don't feel comfortable during the process. And the response by banks and technology companies vary to a great extent. While some companies have reassuring, fast and receptive procedures in place, some companies lack the necessary measures to support the victims.

One of our case studies, a woman in her 60s from the UK, had her bank account compromised. Thousands of dollars were taken from her account. The experience has left her perpetually anxious.

> *"The fear of crime sometimes is worse than the actual crime itself. It was just being fearful, constantly, of my livelihood just flying out of the bank account at any point in time. So, yes, it did affect me, very much."*
> Patricia, 60s, UK

FIGURE 4.
PROPORTION OF CYBERCRIME VICTIMS EMOTIONALLY AFFECTED BY THE EXPERIENCE WHO FELT...



23. Help Net Security. The emotional impact of cybercrime.2010. Available at: https://www.helpnetsecurity.com/2010/09/08/the-emotional-impact-of-cybercrime/#:~:text=The%20first%20study%20to%20examine,blame%20themselves%20for%20being%20attacked [Accessed 12/10/2020]
24. University of Portsmouth. Victims of Computer Misuse. April 2020. Available at: https://researchportal.port.ac.uk/portal/files/20818541/Victims_of_Computer_Misuse_Executive_Summary.pdf?_ga=2.140027824.2021321981.1589972151-179347394.1589972151 [Accessed 12/10/2020]

2.2. FEELING "POWERLESS"

This process can be alienating for some people. At the end of the day, many victims don't know how they lost their data or how to take it back. As a result, they feel powerless and like everything happens out of their control. Angela is a woman in her 50s living in Denver, US. The bank told her that thousands of sets of shapewear - underwear designed to shape a woman's silhouette - were purchased using her account, and she was being charged for going into an unarranged overdraft. She described how she felt when she was a victim of cybercrime:

> *"I did feel powerless and that stress and anxiety, "What am I going to do?" I was pretty confident that the money would get back, but I was afraid what happens until the money gets back - that was a really anxious time."* Angela, 50s, US

People's experiences with being a victim of cybercrime might change with their age. Since younger people use online spaces more than older age groups, they are more likely to become victims of cybercrime. The age itself does not create a vulnerability on its own. However, older people might struggle more with putting the money they lost to cybercrime back than younger people. And often they feel shame in asking for help from their kids and grandkids.

> *"It's a bit like the stages of grief: people feel angry, then they get really stressed and worried. They may retreat, become less confident and less independent… Some fraud victims just go offline and say, "I don't want to engage with the internet because there are too many threats out there, it's just not for me."*
> Joel Lewis, Consumer and Financial Service Policy Manager, Age UK

BEST PRACTICE

EXAMPLE 1: ENHANCED VICTIM CARE (UK)

In the UK, we identified the example of the National Economic Crime Victim Care Unit (NECVCU), run by City of London Police, as an example of best practice.[25] This model uses specialist officers to communicate with and provide advice to victims, based upon their needs and vulnerabilities.[26] As noted by the City of London Police: "After an initial pilot in London, the service is gradually rolling out nationally. The NECVCU team has now expanded to a telephone service in the West Midlands and Greater Manchester."[27]

This model offers victims a far better service, with tailored guidance and support from police forces. Indeed, Joel Lewis, Consumer and Financial Service Policy Manager at Age UK, stressed its value for supporting vulnerable people:

"There's the Economic Crime Victim Care Unit sitting within the City of London Police. I've spoken to the people who run that and work in that and they do good work helping vulnerable and often older victims of fraud and cybercrime too."

By contrast, the most recent ONS data suggests that 50% of people who report cyber fraud to Action Fraud are dissatisfied with their experience.[28] This suggests that these units could solve a wider problem:

"At the moment it's only available to people who live in a handful of police forces, so there's a bit of a postcode lottery. We want to see more funding for that so that can be rolled out across England and Wales." Joel Lewis, Consumer and Financial Service Policy Manager, Age UK

By targeting interventions to support people who have been victimised by fraud, you provide a better service to often vulnerable victims and create a stronger incentive to report crime.

25. Action Fraud. National Economic Crime Victim Care Unit (NECVCU). 2020. Available at: https://www.actionfraud.police.uk/economic-crime-victim-care-unit-ecvcu [accessed 12/10/2020]
26. Interview, Alex Rothwell.
27. Action Fraud. National Economic Crime Victim Care Unit (NECVCU). 2020. Available at: https://www.actionfraud.police.uk/economic-crime-victim-care-unit-ecvcu [accessed 12/10/2020]
28. ONS. Nature of crime: fraud and computer misuse. 2020. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse. [accessed 12/10/2020]

2.3. SHAME AND STIGMA AROUND BEING A VICTIM OF CYBERCRIME

Kristin Judge from Cybercrime Support Network describes that many victims of cybercrime do not come forward to share their stories because of the stigma attached to it. Judge compares this to the shame and stigma victims of domestic violence in the US feels:

> *"There is real shame attached to this crime. If you asked me, can I get a victim to come and speak to you about what's happened to them, I would say no. It's difficult to find victims that are willing to talk about it, because there's a shame and a stigma attached to it. I parallel it to what happened with domestic violence in the US."*
> Kristin Judge, CEO,
> Cybercrime Support Network

The stigma can be even stronger with older victims of cybercrime. The digital tools which younger people find intuitive might be completely new to some older people. For many people who are not 'digital natives', support is often required in accessing online spaces.

> *"We know sometimes family and friends can be reticent to help older people because it can be frustrating. That experience of helping an older relative to use a bit of technology can be frustrating for both people on both sides."*
> Joel Lewis, Consumer and Financial Service Policy Manager, Age UK

For older people, the stigma they face reflects this experience. Given the frustration they can face when trying to gain support from digital natives, they don't want to look like they can't go online or have been tricked into becoming a victim of cybercrime. As Joel Lewis puts it: *"They seek to maybe blame the person rather than understanding the specific factors that led to them becoming a victim in the first place."*

And yet, the participants who consider themselves technology savvy or digitally literate had a greater shame attached to being a victim of cybercrime. Christopher is in his 30s and works at an IT in a bank. His financial information was compromised and someone bought Apple gift cards in his name.

It took him weeks to take his money back. He called them twice a day throughout the process, as he worried otherwise his case would "fall through the cracks". Christopher felt angry at himself, as someone "very strict about his logins, [who] had all kinds of alerts set up", to allow this to happen.

We are less likely to blame ourselves when we are mugged in the street or our house was burgled. However, many participants in our study said they blame themselves and feel ashamed about being a victim of cybercrime. They said they felt like "an idiot, dumb for weeks, blame themselves and embarrassed." This shame can even undermine family relationships.

> *"You might be frightened to tell your partner because you've lost £18,000, you've lost your life savings, you may be frightened to tell her that or him that."*
> Wayne Stevens, Fraud Lead, Victim Support

Romance scams especially have the most devastating emotional impact on the individuals, according to Kristin Judge. Millions of people turn to online dating sites and apps to find romance - perhaps now more than ever before in the time of social distancing. A romance scam happens through gaining the confidence of the victim over time. They invest their time to build a genuine-looking relationship with their victim.

> *"The criminals really convince someone that they're in love with them, so there's emotional control and emotional investment that the victims put into the relationships. Victims can lose their entire life savings. The amount of shame that comes with "I am now 78 years old and I have no money left to support myself." That's a very difficult place to be."*
> Kristin Judge, CEO,
> Cybercrime Support Network

Joel Lewis also mentioned the long-term impact of being a victim to romance scams. It can cause real harm to the health and wellbeing of victims, he said:

> *"It can get so bad with romance fraud that people realise they're being scammed and still continue to give them money because they want to believe the relationship is genuine in some way."*
> Joel Lewis, Consumer and Financial Service Policy Manager, Age UK

2.4. LONG-TERM IMPACTS ON HEALTH

We often miss the connection between the psychological harm and the long-term physical harm due to being a victim of cybercrime. The stress and worry over money or personal data breaches can cause people to lose their sleep, appetite, or gain weight.[29] Some research also identified a link between being a victim of cybercrime and anxiety and depression.[30]

Alex Rothwell from the City of London Police underlined the importance of acknowledging the long-term harm facing some victims:

> *"We know there is huge psychological harm. We've got examples of where there have been suicides."* Alex Rothwell, Deputy National Coordinator of Fraud and Economic Crime, the City of London Police

However, research on the impact of cybercrime victimisation in terms of long-term health implications is quite limited. A study by the University of Portsmouth found that among those victims noting any impact (great or fair amount) 23% reported self-harm and 20% experienced suicidal thoughts.[31] Joel Lewis, Consumer and Financial Service Policy Manager from Age UK, said that the empirical data shows that, in some cases, being a victim of cybercrime can indeed have serious long-term health consequences. He also highlighted that some victims who had contacted Age UK ended up in long-term care, as a result of being a victim of cybercrime. The limitations of literature shows us that more research is necessary, in order to have a holistic understanding of the true cost of cybercrime.

2.5. FEELING VULNERABLE

These emotions of anger, anxiety and worry leave their place to a feeling of vulnerability. And that feeling stays with the victim; it doesn't end when your data has been secured again or money is returned.

Matt, a victim in his 40s from the UK, had his online identity stolen. One night, while he was out with friends, he noticed a message from the UK Government saying "You've got a tax rebate of £900." Within an hour they took approximately £1,000 from his accounts. It was a "long, long process" to get the money back. It was a "nightmare". Even though his card was cancelled, because they had his sort code and name, they were able to continue taking money as direct debits. At the end he was able to take his money back, but like many others, he still feels vulnerable:

> *"I know somebody out there has got my number, has got my address. That does make me a little bit uneasy. Since then, I've doubled security at my house, put cameras everywhere, bars on the door and everything else."* Matt, 40s, UK

For many of the victims, this feeling comes with the idea that no one is really safe from being a victim of cybercrime.

We spoke with Dorothy, a woman in her 60s from the UK. She is very close with her aunt, an 87 year old lady, who lives alone and has been unwell for a number of years. Dorothy's aunt wanted to fly to Australia to see her sister before she passed away, but to be able to travel, Dorothy's aunt required expensive breathing apparatus. The seller seemed legitimate, demonstrating an extensive and convincing understanding of the product. However, after paying the upfront installment fee and waiting a number of days, the equipment hadn't arrived. Dorothy has found herself in a battle to try to reclaim some of her aunt's lost money.

After a dreadful five weeks, not only had Dorothy lost out on the money trying to buy the device, but her aunt's trip to Australia had been cancelled, leaving her emotionally damaged and at a significant financial loss for flights. Going through this experience destroyed both Dorothy's and her aunt's confidence:

> *"She doesn't trust anyone anymore. She thinks everyone's out to scam her. She's paranoid now. She was really outgoing, even though she was ill. But now she's a shell of herself, she's not the same lady."* Dorothy, 60s, UK

Maybe because of this fatalistic idea that no one is safe or because victims usually don't learn how they were hacked in the first place, many said they didn't change their attitudes towards online space after being a victim. The study by University of Portsmouth also found cyber-security behaviours did not seem to change considerably after

29. University of Portsmouth. Victims of Computer Misuse. April 2020. Available at: Plhttps://researchportal.port.ac.uk/portal/files/20818541/Victims_of_Computer_Misuse_Executive_Summary.pdf?_ga=2.140027824.2021321981.1589972151-179347394.1589972151 [accessed 12/10/2020]
30. Ibid
31. Ibid

becoming victim to cybercrime.[32] The research team noted "a small increase in use of device passcodes, software updates, data backups and reporting; and a decrease in the use of device and website password managers." **Overall, the majority of victims did not change their online behaviours.**

CASE STUDY – EDWARD

Edward is in his 50s and lives in the UK. He has two young adult children. He's working as a sales manager in a cosmetics company. His identity was stolen a couple of years ago. They used his name to take credit and loans for two years.

Edward didn't notice anything for two years since they created a fake address in his name. He only learned about what was happening because a debt collection company reached him about his unpaid debt of £8,000. When he learned they took loans worth of seventy thousand pounds in his name, he was shocked.

That was the start of an 8-month nightmare of calls to prove his identity was stolen. He contacted the police and reported this as a cybercrime.

"It was stressful, because however much you're innocent and you know you are, you've got to prove this to all these different companies that it wasn't you. Then you're thinking, 'Well, if they don't believe me, what happens now?' It was getting on for about £70,000, and where am I going to find £70,000 to pay?"

After going through one of the worst experiences of his life, he is now much more savvy about how to protect himself.

"Knowing my name and my date of birth and my home address and my mobile number, but how much more do they know about me? That was my concern."

His message to people who think no one would put an effort to steal their data or identity would be:

"Well, if they go into my bank account there is nothing in there," they don't want your bank account. That's not what they want. They want you. They want your identity, because you're an upstanding citizen, you've got a decent credit record and from that, they can build on that. They're not looking for the rich people, they're looking for just Middle Joe, who they can run up a credit rating with and get some money from. The chances are, Alan Sugar doesn't keep all his money in his Barclays high street bank account."

32. University of Portsmouth. Victims of Computer Misuse. April 2020. Available at: https://researchportal.port.ac.uk/portal/files/20818541/Victims_of_Computer_Misuse_Executive_Summary.pdf?_ga=2.140027824.2021321981.1589972151-179347394.1589972151 [accessed 12/10/2020]

CHAPTER 3
THE CURRENT SYSTEM AND WHY IT IS NOT FIT FOR PURPOSE

KEY FINDINGS

- In the UK and US, **we need fundamental change across law enforcement and victim support systems to better serve people who experience cybercrime.**
- Top-level law enforcement have the capability to tackle complex cybercrime, but lack the capacity (or resources) to do so, suggesting additional resources are needed.
- Local police lack both the capability and capacity to investigate cybercrime, yet are often tasked with handling these kinds of cases. **As a consequence, less than 1% of annual cyber incidents in the US lead to an arrest, let alone prosecution.**[33]
- Action Fraud is not trusted by the British public and requires significant reform - 50% of people who report cyber fraud to this body are dissatisfied with their experience.[34]
- Cybercriminals are agile and innovative, selling and sharing technology and criminal tools quickly via the 'cybercrime as a service model' - the police struggle to keep up.
- **Overall, victims receive an inadequate response: their cases are rarely investigated, cybercrime runs rampant, and victim care is extremely limited.**

"Someone once said that in policing, if it's not shouting, bleeding or banging, then it won't get prioritised."
Rick Muir, Director of the Police Foundation

In the first part of this chapter, we explore the policy landscapes in the US and UK, highlighting their comparative strengths and weaknesses. The Great Cyber Surrender identifies a critical failing within the current approach, whereby local law enforcement are often responsible for tackling cybercrime but lack the expertise to do so, leaving individual victims liable for confronting these incidents. In this chapter, we build on this theme, examining the cyber skills gap between law enforcement and cybercriminals, who are extremely agile and innovative digital actors. We also address the challenges posed by COVID-19 and Brexit to our current cybercrime response.

3.1. POLICY LANDSCAPE

3.1.1. UK

3.1.1.1. National Agencies and Policing

In the UK, the response to cybercrime is guided by the 2016-21 National Cyber Security Strategy, with three different tiers of law enforcement responsible for handling this problem.[35]

33. Peters, A. and Jordan, A. Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. Third Way, 2019. Available at https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime [accessed 14/10/2020]
34. ONS. Nature of Crime: Fraud and Computer Misuse - Dataset (year ending March 2020). 2020. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse [accessed 14/10/2020]
35. As noted in the Introduction, any variation of the term 'UK policing' found throughout this report refers to England and Wales alone - as Scottish and Northern Irish policing is devolved.

The highest level response involves the National Cyber Crime Unit (NCCU) at the National Crime Agency and the work done by the National Cyber Security Centre (NCSC). The NCCU leads and coordinates the national-level response to cybercrime, dealing with critical cyber incidents, rather than smaller fraud cases.[36] By contrast, the NCSC is a more public-facing organisation, providing a single point of contact for businesses and consumers, acting as a source of expertise on cyber security.[37] Our expert interviewees were generally highly supportive of the work done by this body.[38]

The second level of response involves bodies directly responsible for dealing with fraud. Foremost amongst these is Action Fraud, the UK's cybercrime and fraud reporting centre, which is run by the City of London Police working alongside the National Fraud Intelligence Bureau (NFIB).[39] Action Fraud collates cybercrime and fraud reports, before passing some cases onto police forces for investigation.

We find that Action Fraud is not trusted by the British public and requires significant reform. Half of the people who report cyber fraud to Action Fraud are dissatisfied with their experience, according to the most recent ONS data.[40] An investigation by the Times found that more than half of the cases submitted to Action Fraud are not deemed worthy of further investigation by an algorithm, before they have even been seen by a human investigator.[41] Our experts generally agreed that victims were not adequately supported by this organisation. It even has its own parody Twitter account, @InactionFraudUK, with the bio: "We listen to victims of fraud and then ensure nothing is done for them. Our advisors ignore you Mon-Fri." [42]

These failings are partially a function of inadequate resourcing.[43] There is also a lack of clarity about Action Fraud's purpose, which stems from its initial design. Action Fraud was created to collect information, rather than investigate crime:

> *"I think the fundamental problem at the beginning of all of this was that Action Fraud was viewed not so much as a victim service, but as a data collection point."*
> Rick Muir, Director of the Police Foundatio)

Finally, the lowest level of response is within UK police forces, which are handed cases for investigation by Action Fraud. The most sophisticated cases can be handled by the new cybercrime units which have recently been introduced, within the ten Regional Organised Crime Units (ROCUs) spread across England and Wales.[44]

However, beyond these ROCU units, there is little relevant expertise. Two specific issues undermine the local response. First, very few cases are handed down by Action Fraud - a police force in the South of England recently complained that they had received just 10 cases, out of the 600-650 cybercrime reports from their area each month.[45] This means that most cases receive no significant investigative time. Secondly, even if cases were passed down, the lack of resources and expertise amongst police officers at this local level means victims of fraud tend to receive little effective investigation anyway.

Crucially, there are some exceptions to this, namely Economic Crime Victim Care Units (ECVCUs), which provide tailored support and advice. Our expert from Age UK highlighted the value that these units offer to vulnerable people who have been victimised by cybercrime.[46] However, the availability of these units is extremely limited, meaning that there is something of a 'postcode lottery' for victims in the UK, at present.

But generally, police are focused on tackling more traditional and violent forms of crime, and neglect cybercrime cases. As the quote that leads this chapter acknowledges, fraud does not involve any obvious 'shouting or bleeding or banging'.[47]

36. National Crime Agency. What We Investigate - Cyber Crime. 2020. Available at https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime [accessed 14/10/2020]
37. HM Government. National Cyber Security Strategy 2016-2021. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [accessed 14/10/2020]
38. Interviews, Michael Levi; Ingolf Becker; Mark Montgomery and Rob Morgus.
39. Action Fraud. Who are the National Fraud Intelligence Bureau?. 2020. Available at https://www.actionfraud.police.uk/what-is-national-fraud-intelligence-bureau [accessed 14/10/2020]
40. ONS. Nature of Crime: Fraud and Computer Misuse - Dataset (year ending March 2020). 2020. Available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse. [Accessed 14/10/2020]
41. Sanderson, D. Computer says no to police action in cyberfraud cases below £100k. The Times, 2020. Available at https://www.thetimes.co.uk/article/computer-says-no-to-police-action-in-cyberfraud-cases-below-100k-znsvwcp3s [accessed 14/10/2020]
42. @inactionfrauduk. InAction Fraud. 2020. Available at twitter.com/inactionfrauduk [accessed 14/10/2020]
43. Interview, Ingolf Becker.
44. Interview, Alex Rothwell.
45. Nixon, G. Action Fraud 'failing to hand over cases to the police for investigation'. This is Money.co.uk, 2019. Available at https://www.thisismoney.co.uk/money/beatthescammers/article-7538323/Senior-police-officer-says-Action-Fraud-doesnt-police-cases-investigate.html [accessed 14/10/2020]
46. Interview, Joel Lewis.
47. Her Majesty's Inspectorate of Constabulary and Fire & Rescue Service. Fraud: Time to Choose - An Inspection of the Police Response to Fraud. 2019. Available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/fraud-time-to-choose-an-inspection-of-the-police-response-to-fraud.pdf [accessed 14/10/2020]

As a consequence, this crime is often ignored by police forces, in favour of crimes which involve more obvious or public forms of harm:

> *"In terms of local policing, fraud will never be prioritised. You could try to force the local forces to do more, but I came to the conclusion that that was just a fool's errand."* Rick Muir, Director of the Police Foundation

3.1.1.2. International Collaboration

The UK has historically worked closely with international partners in digital law enforcement. Within Europe, this collaboration has often occurred through Europol, which unites Europe-wide law enforcement agencies to tackle high-level crime. Importantly, the Brexit process calls into question how close this cooperation can be in the future:

> *"We need to find a way of developing an effective relationship with Europol, post-Brexit…"* Alex Rothwell, Deputy National Coordinator of Fraud and Economic Crime, City of London Police

> *"We're leaving Europol. So, first, we lose the European Arrest Warrant, which massively fast-tracks our ability to apprehend suspects in other countries. We also lose crucial access to databases and intelligence…"* Rick Muir, Director of the Police Foundation

Beyond Europe, law enforcement collaboration is highly variable, reflecting existing tensions and alliances in international politics. Thus, UK agencies collaborate very closely with US law enforcement, as exemplified by the 2019 signing of the Cloud Act, which streamlines data sharing about serious crime across jurisdictions.[48] By contrast, collaboration with some states is non-existent, particularly those which turn a blind eye to some cybercriminal activity:

> *"Law enforcement are not going to be able to arrest them. That's fantasyland. They live in Russia and they're not getting extradited…"* Sherrod DeGrippo, Senior Director of ProofPoint

> *"If the offender is in Russia or China... there's no point in trying to pursue them, unless it's a really big case, because the countries simply won't cooperate."* Professor Michael Levi, Cardiff University

3.1.1.3. Private Sector Collaboration

In terms of the quality of collaboration with the private sector, we found mixed evidence in the UK. The NCSC, the UK's public-facing body for helping support businesses to manage cyber threats, is fairly well-regarded and effective. Indeed, one US expert, Mark Montgomery, contrasted it favourably with the equivalent US capability for coordinating private-public cybersecurity work.

In addition, we identified examples of industry partners working closely with law enforcement to tackle specific cybercriminal threats. This even extended to private funding for some law enforcement capabilities:

> *"We have a number of units that are funded or part-funded by the private sector – a dedicated card payment crime unit, an insurance fraud unit..."* Alex Rothwell, Deputy National Coordinator of Fraud and Economic Crime, City of London Police

And yet, some interviewees also expressed their view that financial institutions could be doing more to help tackle cyber fraud:

> *"Ideally, I think we need an automated process, so that every time you ring your bank about fraud, there is a simple process that allows us to obtain information about what happened."* Alex Rothwell, Deputy National Coordinator of Fraud and Economic Crime, City of London Police

> *"If you use PayPal, you have 30 days to make a claim and have a payment reversed. But if I make a payment to you from my bank, they will tell me it is impossible to reverse this transaction, even if I can prove that you scammed me."* Dr Ingolf Becker, University College London (UCL)

3.1.1.4. Conclusion

Overall, there are three primary strengths to the UK's approach. First, the NCSC, a highly-regarded and effective organisation, which provides information and support to the public in dealing with cyber threats.

Second, law enforcement capability has improved in the UK, to some extent. The development of a cybercrime unit within every police force, often nested within ROCUs, is clearly a valuable step

48. Department of Justice - Office of Public Affairs. US and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online. 2020 Available at https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists [accessed 14/10/2020]

towards enhancing police cyber capabilities. While Scottish policing is managed by the Scottish Government - and is separate from UK policing more broadly - the announcement of a new cybercrime centre by Police Scotland also exemplifies the growing desire for an enhanced cyber capability.[49]

Similarly, ECVCUs, which provide victim care, are useful tools - although they are in place in relatively few forces, at present.

Finally, collaboration with private businesses is generally positive. While several interviewees suggested banks should do more to help tackle cybercrime, forces like the City of London Police are benefiting from strong relationships with private sector stakeholders.

However, there are three major weaknesses to the UK's response. First, the UK's history of effective international collaboration is clearly under threat. Europol has done excellent work confronting cybercrime - and the UK has played a key role in developing it.[50] Post-Brexit, the UK government must ensure that security and policing collaboration with Europe is protected, to ensure we retain access to vital intelligence and investigations.

Secondly, victims of cybercrime deserve a better service. While ECVCUs are extremely positive, victim care is often entirely absent in the British system. Given the emotional impact of these crimes, as Chapter 2 explains in more detail, the current victim care system is clearly not fit for purpose. The statistics bear this out - half of victims reporting cyber fraud to Action Fraud are dissatisfied with their experience.[51]

Finally, the UK needs a better system to handle investigations. In the UK, local police are rarely passed cases by Action Fraud; even if they are, they usually lack the expertise to investigate these crimes. What this means is that the majority of cybercrime cases are not investigated properly; when you consider that victim care is largely absent too, it becomes clear that the current system treats victims extremely poorly.

3.1.2 US

3.1.2.1 National Agencies and Policing

In terms of national-level agencies, the current US infrastructure for tackling cybercrime is far less effective than that of the UK. The US equivalent of the NCSC is the Cybersecurity Infrastructure Security Agency (CISA), a body based within the Department for Homeland Security.[52] CISA is responsible for coordinating nation-wide cybersecurity, but lacks the capability to effectively complete this task:

> *"... [CISA] lacks the ability to direct other federal agencies in their efforts. So at the operational level, our primary agency is not properly enabled."* Mark Montgomery, Executive Director of the Cyberspace Solarium Commission

Similarly, the National Cyber Communications Integration Centre (NCCIC), responsible for sharing information with the private sector, is ineffective. In the words of one interviewee, Rob Morgus, it "barely exists." As a consequence, national-level leadership around cybercrime is extremely limited.

Below these organisations is the Internet Crime Complaint Center (IC3), a reporting hub run by the FBI - akin to the UK's Action Fraud.[53] IC3 reviews complaints, before passing them to relevant law enforcement bodies for investigation or enforcement action. **As in the UK, underreporting is a problem, with the head of IC3 stating in 2016 that they only capture 10-12% of the true scale of cybercrime victimisation.**[54]

The US possesses some pockets of sophisticated cyber capability. In particular, the National Cyber Investigative Joint Taskforce (NCIJTF), housed in the FBI, integrates cyber expertise from law enforcement, defence and intelligence agencies, to provide expert investigation and analysis.[55] However, this body could benefit from additional resourcing:

49. BBC News. New Scottish Police Centre to Tackle Cyber Crime. 2020. Available at https://www.bbc.co.uk/news/uk-scotland-54309549 [accessed 14/10/2020]
50. Interview, Rick Muir.
51. ONS. Nature of Crime: Fraud and Computer Misuse - Dataset (year ending March 2020). 2020. Available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse [accessed 14/10/2020]
52. Cybersecurity Infrastructure Security Agency. About CISA. 2020. Available at https://www.cisa.gov/about-cisa [accessed 14/10/2020]
53. Internet Crime Complaint Center. IC3 Mission Statement. 2020. Available at https://www.ic3.gov/about/default.aspx [accessed 14/10/2020]
54. Baker, A. An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported. New York Times, 2018. Available at https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html [accessed 14/10/2020]
55. United Nations Office of Drugs and Crime. E4J University Module Series - Module 5: Cybercrime Investigation. 2019. Available at https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/who-conducts-cybercrime-investigations.html [accessed 14/10/2020]

"'Does the FBI have the skills and capabilities?' Yes. 'Do they have the capacity?' I think they would say no, they need more." Mark Montgomery, Executive Director of the Cyberspace Solarium Commission

By contrast, local law enforcement in the US faces the same problems as UK police forces. Local police again lack the skillset to deal with even the most basic forms of cybercriminal activity.[56] This is partly because of the cost involved in hiring, training and retaining digital-savvy police officers, but also reflects the emphasis placed by local law enforcement on traditional forms of crime that involve 'shouting, bleeding or banging'. **This leads to a pronounced failure to successfully investigate cases; a recent study found that less than 1% of the cyber incidents that occur annually in the United States result in an arrest.**[57] Our experts concurred with this assessment:

"Most local law enforcement agencies don't have the staff or necessary training." Kristin Judge, CEO of the Cybercrime Support Network

"...they do not have the right skills and they do not have enough of the right people." Rob Morgus, Senior Director of Cyberspace Solarium Commission

3.1.2.2. International Collaboration

In general, US law enforcement has been effective at leading international collaboration around cybercrime. The US has a close relationship with its UK counterparts, having signed a data-sharing agreement under the Cloud Act.[58] The US also has a strong record leading international law enforcement agencies in large-scale cybercrime investigations, as evidenced by the Infraud indictment in 2018.[59] Indeed, this work offers valuable information to private cybersecurity firms too, as they seek to design their strategies for combating cybercriminal threats.[60]

However, international collaboration on cybercrime has faced some strain, due to tensions between the US and its allies in the Trump era:

"...in the US, we have spent a lot of time alienating our traditional allies on trade, and on other issues. That has an effect. It makes it harder get political commitments to work on transnational issues together" Chris Painter, GFCE Foundation

Despite this challenge, collaboration has been relatively robust, because law enforcement agencies are usually keen to work with their international counterparts:

"The politics hasn't infected collaboration too much, because law enforcement is good at talking to law enforcement… Their head is down and they care about this…" Chris Painter, President of the GFCE Foundation

3.1.2.3. Private Sector Collaboration

By contrast, collaboration with the private sector is highly inadequate within the United States:

"...we lack the infrastructure for building public-private collaboration. We do not have a joint cyber planning office, we do not have a joint collaborative environment, and we do not have an integrated command, control and communications centre." Mark Montgomery, Executive Director of the Cyberspace Solarium Commission

This absence places significant limits on the value that the US government can offer to private partners. While some US law enforcement actors could tackle digital crimes alone, the absence of the private sector means missing out on additional capabilities:

"Often the business community can have tools, data or resources that the law enforcement community doesn't." Chris Painter, President of the GFCE Foundation

"If you go to some of our banks - JP Morgan, Morgan Stanley, etc., they potentially have more mature cyber operations than the US government does." Rob Morgus, Senior Director of the Cyberspace Solarium Commission

56. Aguilar, E. Local law enforcement struggle to keep up with cybercrime. Southern California Public Radio, 2014. Available at https://www.scpr.org/news/2014/04/25/43714/report-local-law-enforcement-struggle-to-keep-up-w/ [accessed 14/10/2020]
57. Peters, A. and Jordan, A. Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. Third Way, 2019. Available at https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime [accessed 14/10/2020]
58. Department of Justice - Office of Public Affairs. US and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online. 2020 Available at https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists [accessed 14/10/2020]
59. Department of Justice - Office of Public Affairs. Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes. 2018. Available at https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible [accessed 14/10/2020]
60. Interview, Sherrod DeGrippo.

The challenge in the US is therefore even more fundamental than resourcing law enforcement. The US needs to develop the kind of sophisticated, national-level cyber infrastructure required for ensuring effective private-public collaboration. In short:

> *"...what the US government can do better is be a mature partner for the private sector"* Rob Morgus, Senior Director of the Cyberspace Solarium Commission

3.1.2.4. Conclusion

Overall, the US response to cybercrime is highly inadequate, as things stand, offering a poor service to victims and imposing unhelpful limits upon valuable public-private collaboration.

Nonetheless, there are two strengths to the US' current approach to dealing with cybercrime, First, US law enforcement agencies are extremely effective at collaborating with international peers to tackle large-scale cybercrime networks. An example of this is the Infraud indictment of 2018, which involved collaboration with policing counterparts in the UK, Serbia and Australia, amongst others.[61] Our US-based private sector expert also commended these efforts.[62]

Secondly, these law enforcement efforts appear resilient enough to weather significant political pressure. As Chris Painter noted, despite tensions between the US and its allies during the Trump era, its law enforcement agencies have continued to work closely and effectively with their international allies.

The weaknesses of the US approach are far more pronounced. First, the US' national-level cyber infrastructure is clearly inadequate. In contrast to the UK's NCSC, corresponding US bodies (like CISA and the NCCIC) are limited and ineffective central bodies. This creates a second weakness - a lack of effective private-public collaboration. Opportunities for businesses to work with government and law enforcement to protect consumers are being routinely missed.

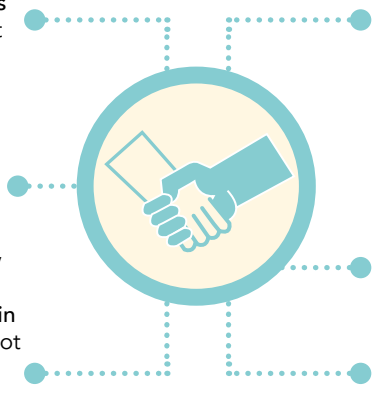
In addition, as in the UK, cybercrime victims in the US receive a poor service from the criminal justice system, with less than 1% of cyber incidents leading to an arrest.[63] Local law enforcement clearly lack the skills required to investigate these crimes, meaning that citizens are often left without appropriate support or guidance, let alone effective resolutions of their cases. Ultimately, the US needs to substantially reform its current approach to dealing with cybercrime.

TRUST AND WHO IS RESPONSIBLE?

Almost two thirds of Britons (59%) **and more than half of Americans (55%)** agreed with the statement "The government is not doing a good job of protecting people from online fraud."

60% of the UK public and 61% in the US agree that "Most online fraud could be solved if the government, companies and individuals put their minds to it."

45% of the UK public (and 45% in the US) believe companies are not doing enough to keep people's data secure.



Six in ten Americans (61%) think most online fraud could be solved if the government, companies and individuals put their minds to it.

The majority of Britons (63%) and Americans (55%) believe the legal system is not doing enough to protect people from online fraud.

In the most recent ONS report, figures showed that 50% of people who report cyber fraud to Action Fraud are dissatisfied with their experience.'

61. Department of Justice - Office of Public Affairs. Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes. 2018. Available at https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible [accessed 14/10/2020]
62. Interview, Sherrod DeGrippo.
63. Peters, A. and Jordan, A. Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. Third Way, 2019. Available at https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime [accessed 14/10/2020]

BEST PRACTICE

EXAMPLE 2: A NATIONAL CYBERCRIME REPORTING HOTLINE, '119' (ISRAEL)

In Israel, victims of cybercrime are able to report incidents to the government's Computer Emergency Response Center (CERT), via a dedicated '119' phone number, set up in 2019.[64] This service is provided 24 hours a day, 7 days a week, and provides a triage capacity to any affected entity - offering support and advice when anyone is the victim of a cybercrime.

Importantly, this service relies on investment of sufficient resources to handle complaints and reports. Despite the costs this would involve, several of our US interviewees suggested this idea might be worth adopting by their own government too.[65] This is because victims are often unsure how to report cybercrime, or believe that reporting will lead to no response from government or police forces.

Of course, Action Fraud, the UK's dedicated fraud reporting centre, does have its own, longer phone number. But the 119 number is far clearer - it provides an easy, recognisable three-digit phone number, to streamline reporting for victims of cybercrime and fraud.

3.2. THE CYBERSECURITY SKILLS GAP

The Great Cyber Surrender reveals a stark asymmetry in skills between criminals and law enforcement. Law enforcement has limited cyber expertise, leaving it unable to deal with the agility and creativity of cybercriminal activities. More specifically, while top-level law enforcement has some capability to tackle cybercrime, it lacks the capacity (or resources) to do so. By contrast, local law enforcement is even more limited, lacking even the capability to seriously engage with these forms of crime, let alone the capacity. This issue is further exacerbated by two contemporary challenges: the COVID-19 pandemic and the possible implications of Brexit.

3.2.1. Cybercriminal Agility

For law enforcement, even keeping pace with criminal behaviour is extremely difficult. This inability to keep up can even extend to legal frameworks, with some judges raising concerns in 2016 that the US legislation for prosecuting cybercrime was itself inadequate.[66] By contrast, cybercriminals have a constantly changing modus operandi, reacting quickly to exploit new opportunities to deceive or target victims:

> *"Fraudsters are very innovative. Criminals are very innovative. They'll always develop new tactics to take money from people."* Joel Lewis, Consumer and Financial Service Policy Manager at Age UK

This innovation is enhanced because new technological developments are shared very rapidly across criminal marketplaces. For example, cybercriminal tools, such as malware, can be purchased online and deployed by criminals, even if they lack great technical skills.[67] This is often termed the 'cybercrime as a service' model, as one expert explains:

> *"[There is] this increasing movement to cybercrime as a service model for a lot of threat groups. Where, basically, these criminal enterprises run as businesses that exchange code and exchange tactics and procedures for money, on the dark web and on the deep web, which is causing this massive proliferation of capability to conduct cybercrime."* Rob Morgus, Senior Director at the Cyberspace Solarium Commission

This criminal agility means those tasked with confronting cybercrime are left playing whack-a-mole. Cybercriminals attempt to evade detection by law enforcement, cybersecurity firms and spam filters; when they are eventually caught, they adapt again, trying new methods and pathways to reach victims. As one cybersecurity analyst told us:

> *"In the morning, everything's working great and we can see what's going on. Then, by the afternoon, somebody on my team will say, "I can't get this to execute anymore"…*

64. Government of Israel. The Israeli Cyber Emergency Response Team (CERT). 2020. Available at https://www.gov.il/en/departments/news/119en [accessed 14/10/2020]
65. Interviews, Mark Montgomery and Kristin Judge.
66. Williams, K. B. Judges Struggle with Cyber Crime Punishment. The Hill, 2016. Available at https://thehill.com/policy/cybersecurity/265285-judges-struggle-with-cyber-crime-punishment [accessed 14/10/2020]
67. Schwartz, M.J. Cybercrime-as-a-Service Economy: Stronger Than Ever. Bank Info Security, 2016. Available at https://www.bankinfosecurity.com/cybercrime-as-a-service-economy-stronger-than-ever-a-9396 [accessed 14/10/2020]

The adaptation is very rapid."
Sherrod DeGrippo,
Senior Director of ProofPoint

And another part of why these criminal activities are so effective is that the risk factors involved are growing more quickly than the amount of resources we are willing to invest in our security. We are ever more reliant upon technology, upon the digital tools which expose us to cybercriminals, meaning that:

> *"The availability of increasingly sophisticated tools to non-state actors is increasingly exponentially, as is the interconnectivity of our systems. So, your two big risk factors are increasing exponentially. Our investment in cyber defence is linear, and, at best, a slight upslope."* Mark Montgomery, Executive Director of the Cyberspace Solarium Commission

> *"Cybercrime can also be about theft and use of data. As more and more data is generated about our daily lives and as it becomes more and more valuable, this data will be targeted by cybercriminals."* Joel Lewis, Consumer and Financial Service Policy Manager at Age UK

Victims and the law enforcement agencies tasked with protecting them, therefore, face an extraordinarily adaptable, innovative and multi-faceted cybercriminal threat. Criminals and fraudsters are constantly updating their methods to target our vulnerabilities, but they can also quickly disseminate these tools - such as malware via digital marketplaces - through the 'cybercrime as a service' model.

3.2.2. Skills Gap - Capability vs Capacity

Law enforcement possesses a far more limited cyber skillset, in comparison to the fraudsters and cybercriminals they are charged with investigating. This deficiency ultimately occurs in two different ways. Top-level law enforcement often do have the capability required to deal with complex cases, but they lack the capacity to do so at scale. By contrast, local police forces face a more fundamental problem: they have very little capability to investigate cybercrime, let alone the capacity to do so on a routine basis.

In the UK, it is clear that some law enforcement bodies do have an advanced cybercrime capability. For example, the National Cyber Crime Unit housed within the National Crime Agency. Furthermore, at the regional level, there is a network of cybercrime squads within the ten Regional Organised Crime Units (ROCUs) spread across England and Wales, which also provide access to some specialist cyber capabilities.

By contrast, most local police forces lack the resource capability to deal with cybercrime, and particularly fraud offences, in an effective way.[68] For example, a 2018 study found that police officers were even confused about the meaning of the term 'cybercrime' and exactly what offences it might include.[69] This demonstrates that local police officers in the UK lack the capability and requisite expertise, let alone the capacity, to deal with cybercrime.

In the US, we can see a similar picture. At the national level, there are law enforcement bodies with the advanced capability required to investigate cybercrime - but they lack sufficient capacity to do so:

> *"'Does the FBI have the skills and capabilities?' Yes. 'Do they have the capacity?' I think they would say no, they need more."* Mark Montgomery, Managing Director of the Cyberspace Solarium Commission

By contrast, local law enforcement within the US is lacking in both capability and capacity:

> *"At the state and local level, they do not have the right skills and they do not have enough of the right people."* Rob Morgus, Senior Director at the Cyberspace Solarium Commission

It's important to remember the impact of this skills gap on victims of crime. In the US, less than 1% of the cyber incidents that occur annually result in any arrest, let alone a successful prosecution.[70]

Ultimately, there is a clear skills gap between UK-US law enforcement and the agile, innovative threats posed by cybercriminals. In both countries, local officers lack the capability to investigate lower-level cybercrimes and, although national law enforcement has some cyber capability, it lacks

68. RPC. Hacking Prosecutions Fall for a Further Year Despite the Threat of Cyber. 2020. Available at https://www.rpc.co.uk/press-and-media/hacking-prosecutions-fall-for-a-further-year-despite-the-threat-of-cyber-crime [accessed 14/10/2020]
69. Hadlington, L., Lumsden, K., Black, A., Ferra, F. A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime. Policing: A Journal of Policy and Practice, 2018. Available at: https://doi.org/10.1093/police/pay090 [accessed 14/10/2020]
70. Peters, A. and Jordan, A. Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. Third Way, 2019. Available at https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime [accessed 14/10/2020]

the capacity to investigate these crimes at scale. However, this skills gap is now being exacerbated by the current crisis we face with COVID-19.

3.2.3. COVID-19

The pandemic provides a textbook example of how adaptable this cybercrime threat is. COVID-19 is one of the most socially disruptive events in recent memory. It has created substantial uncertainty and upheaval, which has been carefully exploited by fraudsters and other cybercriminals.

These kinds of conditions are ideal for cybercriminals, who rely on successful 'social engineering' to successfully defraud victims. Social engineering refers to the human component of cybercriminal activity, the emotional manipulation and targeting of human weaknesses which allows criminals to defraud people, rather than the specific code or digital tool involved in any given scam:

> *"...with social engineering, it's all psychological. They want to get you into that emotional, psychological state so that you take an action."* Sherrod DeGrippo, Senior Director of ProofPoint

For example, several interviewees noted the rise of scams related to COVID-19. This is extremely effective social engineering, as it targets a source of deep fear or anxiety amongst people in the current pandemic. For example:

> *"It was around things like getting protective equipment, there were a lot of scams about that in the beginning. Fake masks and fake PPE."* Kristin Judge, CEO of the Cybercrime Support Network

> *"We've seen things like, 'Your invoice for PPE, like gloves, masks, all that, is attached. You need to pay this invoice before we can ship you out your protective equipment.'"* Sherrod DeGrippo, Senior Director at ProofPoint

However, this adaptation is primarily at the front-end of fraudulent activity, reflecting changes in the packaging of scams, rather than their underlying products. It is the social engineering which has been adapted, rather than the technical side of these scams. In other words, cybercriminals have not developed any new methods of defrauding victims, but they have effectively rebranded them to fit the current circumstances:

> *"We haven't necessarily seen any new methodology. Clearly, criminals have used the COVID crisis as a hook, but that's not necessarily new methodology."* Alex Rothwell, Deputy National Coordinator of Fraud and Economic Crime, City of London Police

> *"...the impact has been primarily around the social engineering that is wrapping the attacks… There have been thousands of social engineering styles around COVID-19."* Sherrod DeGrippo, Senior Director of ProofPoint

Thus, fraudsters have adapted their social engineering to tap into and exploit people's most pressing vulnerabilities and anxieties. During the upheaval and uncertainty of a pandemic, the most effective scams are likely to be related to PPE, as opposed to the usual PPI.

An important implication of this agility is that criminals will keep innovating around different crises or large-scale events. For example, on Black Friday and Cyber Monday, fraudsters may repackage their scams as 'deals' or 'time-limited, money-off promotions'. Cyber fraudsters will continually adapt to find the best ways of exploiting victims - law enforcement needs to be more agile and better resources, in order to try and keep up.

Whether COVID-19 has led to an increase in the total level of fraudulent activity is unclear. Some evidence suggests this may be the case: the Internet Crime Complaint Center (IC3), the US body responsible for collating reports of cybercrime, stated that its usual 1000-complaints a day caseload had increased to 3000-4000 cases a day during April.[71] Our polling also found that a majority of people in the UK and US perceived that fraud had become a greater problem since the start of the pandemic. In addition, data from the Federal Trade Commission (FTC) states that they have received over 117,000 reports of COVID-related fraud, amounting to over $60 million lost by US consumers, as of October 2020.[72] Some further evidence is the recent announcement of a new business fraud reporting line, launched by Crimestoppers in the UK.[73]

However, there are reasons to be sceptical about this. Throughout our interviews, several experts suggested that the true effect of COVID-19 on fraud cases was difficult to determine at this stage:

71. Cimpanu, C. FBI says Cybercrime Reports Quadrupled During COVID-19 Pandemic. ZD Net, 2020. Available at https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-COVID-19-pandemic/ [accessed 14/10/2020]
72. Public Tableau. FTC COVID-19 and Stimulus Reports (Fraud Reports). 2020. Available at https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/FraudLosses [accessed 14/10/2020]
73. Makortoff, K. Covid Crimestoppers Hotline Launches to Catch Business Loan Fraudsters. The Guardian, 2020. Available at https://www.theguardian.com/uk-news/2020/oct/13/covid-crimestoppers-hotline-launches-to-catch-business-loan-fraudsters [accessed 14/10/2020]

"...it's a bit unclear what's happened. The latest figures I saw were police-recorded fraud figures, and they didn't seem to show much of an increase when compared to other areas..." Rick Muir, Director of the Police Foundation

"I don't think the consequences have been nearly as big as people expected. But it's difficult to know what would have happened if the National Cyber Security Centre hadn't done anything. In that case, there might have been a lot more." Professor Michael Levi, Cardiff University

Measuring the impact of the pandemic on levels of fraud may become easier in 2021, once more data becomes publicly available. But this should not distract from the key effect of COVID-19: it has acted as a case study for the agility and adaptability of contemporary cybercriminals. In the context of highly limited police cyber capabilities, law enforcement faces a challenging task in trying to keep track of the threats to victims online.

3.2.4. Brexit

A final challenge, specific to the UK, is the Brexit process - specifically, its impact on the effective collaboration needed to help tackle cybercrime. Failing to reach a relevant agreement on security and policing collaboration with the EU is a serious challenge. It would mean that British law enforcement could not be involved in some Europol investigations and would be unable to access European databases containing valuable intelligence:

"Some of the most successful international operations involve joint investigations, run by teams of officers from different countries working across jurisdictions. Europol has pioneered that kind of thing and it's unfortunate that we're dropping out." Rick Muir, Director of the Police Foundation

"...we need to develop an effective relationship with Europol, post-Brexit, that gives us similar access to the information and tools that exist through that process. That will involve collaboration, bringing data together and sharing expertise." Alex Rothwell, Deputy National Coordinator of Fraud and Economic Crime, City of London Police

Failing to obtain a Brexit deal would be a serious issue, which might prevent UK law enforcement from being able to benefit from international collaboration. Given the challenges that have been outlined in this chapter - around cybercriminal agility, the evolving threats seen during COVID-19, and limited law enforcement cyber skills - protecting international collaboration is an important priority for policymakers trying to tackle cybercrime. Looking forward, an effective international agreement with the EU around policing and security cooperation is vital, to help plug the growing cyber skills gap within the UK.

BEST PRACTICE

EXAMPLE 3: COLLABORATING TO TACKLE INFRAUD (2018)

A key priority for US and UK policymakers should be to build an environment where effective international collaboration occurs, so that different agencies work together to protect victims from cybercrime. Given that cybercrime is an agile and transnational threat, building international partnerships to tackle these digital threats is vital. Through international collaboration, different states can learn from each other's experiences, sharing best practice and methods for helping to deal with cybercrime.

A textbook case of this is the 2018 indictment of 36 individuals in connection with the Infraud criminal organisation.[74] This operation involved effective collaboration between law enforcement agencies in the US, Australia, France, UK and Kosovo, amongst others to identify these major criminal actors. Although these actions might not lead to immediate arrests or prosecutions, when they are made public, they also help the private sector mitigate criminal activity too:

"In these cases, law enforcement will take everything they found and put it in the indictment as justification. Then our teams take all that information and use it to create protections..." Sherrod DeGrippo, Senior Director at Proofpoint

74. Department of Justice - Office of Public Affairs. Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes. 2018. Available at https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible [accessed 14/10/2020]

CHAPTER 4
HOW TO FIX IT

In both the UK and the US, *The Great Cyber Surrender* identified a common failure to provide victims of fraud with an effective response. Victims are often confused about the reporting process and are convinced that law enforcement will not be able to help them - and often, they are correct in this belief. This means that cyber fraud is constantly underreported, investigations are rarely completed (or even started), and victims are left to suffer substantial emotional harm from these crimes with little support from government or police. We have a vital opportunity to help resolve this failure, with the UK's National Cyber Security Strategy expiring in 2021 and the start of a new presidential term offering a chance to lobby for change. Therefore, we propose that the US and UK adopt a new National Fraud Infrastructure, involving three components:

Recommendation 1: Government should establish a National Reporting Hotline for fraud and cybercrime, with a simple three-digit number, e.g. '119 for Cybercrime.'

This measure provides a single point of contact for victims of cybercrime and fraud, with a significant public profile and recognisable phone number. A dedicated hotline aids the public in two main ways: (1) it shows that their experiences of cybercrime matter to the government and to law enforcement, and (2) it removes much of the confusion around reporting, which prevents victims from seeking help.

This model is clearly achievable, if sufficient resources were invested by the government. A national reporting hotline already exists in Israel, within its Cyber Emergency Response Center (CERT). In the US, the Cybercrime Support Network is piloting a similar idea, a trial programme to support cybercrime victims, operated via the US' existing 211 phone number which provides a range of support functions.[75] In the UK, this hotline could be implemented via renewing and rebranding Action Fraud. This would be a two-step process, of: (1) rebranding this body, which the public often does not trust, and (2) replacing its longer phone number with a recognisable three-digit alternative.

Recommendation 2: Government should establish a National Fraud Taskforce, staffed with specialist investigators, with responsibility for investigating cyber fraud cases.

But a National Reporting Hotline is only beneficial when newly reported cases receive an effective response from government. In other words, when victims report cases to the National Reporting Hotline, they must always be evaluated to determine if there are any significant investigative leads. If there are, any such cases must be passed to the National Fraud Taskforce, which would be responsible for handling all cybercrime - except those extremely serious cases, which can be handled by agencies like the NCA.

This replaces the current approach, whereby fraud cases are passed to local law enforcement agencies which lack the capability and motivation to investigate them. By contrast, a National Fraud Taskforce, adequately resources and funded, would provide accountability and specialisation for handling fraud cases, offering an improved service to victims. This new body could best be housed within the FBI (US) and the City of London Police (UK).

75. Cybercrime Support Network. Campaigns. 2020. Available at https://cybercrimesupport.org/campaigns/ [accessed 14/10/2020]

Recommendation 3: Government should roll out Victim Care Squads nationally, staffed with specialist advocates, to provide support and advice to victims of cybercrime.

But we also recognise that some fraud cases cannot be investigated effectively - for example, when the perpetrators are based in countries which will not work with UK or US law enforcement, like Russia. However, this does not mean that governments can do nothing to help. Our research is clear - people face substantial emotional harms and even mental health issues when they are victims of cyber fraud, they deserve some kind of response.

Therefore, even when cases cannot be investigated, they should be passed onto specialist Victim Care Squads housed within local police forces. These squads would be required to triage cases and make contact with every victim, offering tailored support and advice on basic prevention measures. This contact could range from a simple phone call, in simple cases, to a full-scale intervention plan for especially vulnerable victims. These squads can be modelled on the Economic Crime Victim Care Units (ECVCUs) currently in place within a number of UK police forces, with a goal of providing local-level emotional support and prevention advice.

We also recommend the following measure, in the UK and US, to ensure businesses play their part in dealing with cybercrime:

Recommendation 4: Banks should have a legal duty to pass anonymised information to the new National Reporting Hotline, whenever their customers are victimised by cyber fraud.

While measures like the 119 hotline should improve rates of fraud reporting, often it is banks that receive the first contact from victims. For example, if someone identifies an unauthorised transaction out of their account, they can contact their bank and the money will be reimbursed. In such cases, police rarely receive a report from the person affected.[76]

Banks should be required to pass on information, whenever customers are victimised, to the National Reporting Hotline. This should include basic information about the crime (the amount lost, account the money was sent to, method of contact, etc), to help police develop a more sophisticated picture of the true scale of the fraud threat. Crucially, this information should be anonymised and shared by the bank through extremely secure channels. People can choose to go to banks to get their reimbursement and not deal with the law enforcement if they don't want to. But this would allow police to use this information as intelligence.

Recommendation 5: Whenever a data breach occurs, businesses should have a legal duty to provide customers with timely, step-by-step guidance on how to protect themselves and must introduce remedial security measures - such as mandatory multi-factor authentication on customer accounts.

In Chapter 2, we noted the severe emotional impact that cybercrime can have upon individuals. Cybercrime victimisation is a disorienting experience, made more confusing by the fact that victims are sometimes provided with inadequate information when their data is stolen from private companies.

We recommend a stronger legal duty, placed upon businesses when they suffer data breaches which result in the loss or exposure of customer data. In these circumstances, companies should have an obligation to provide customers with step-by-step guidance on the precise actions they need to take to protect themselves, their data and their other accounts within a reasonable timeframe. In addition, companies should be required to introduce remedial security measures after such events, in light of the higher risks customers face after their data is accessed illegally. This could include mandatory multi-factor authentication (to prevent illicit or false payments being made) or requiring new, more complex passwords (to ensure user accounts are secured).

We also recommend a series of education measures, designed to teach children effective cybersecurity from a young age, and to encourage adults to change their behaviours online:

76. Interview, Alex Rothwell.

Recommendation 6: Mandate basic cybersecurity education within schools, teaching children about digital literacy and cybercrime, including how to create effective passwords, use multi-factor authentication and identify cyber-scams.

In each of our ten interviews with US and UK experts, we asked: 'If you were providing advice directly to the public, what one measure would you recommend they take to protect themselves from cybercrime?' Time and again, the answers were the same: people must take basic cybersecurity measures - strong passwords, multi-factor authentication, thinking before sending money.

Developing these habits in young people as they first begin using digital devices is vital to help prevent them suffering cyber fraud - in the US, in particular, this kind of education is sorely lacking.[77]

Recommendation 7: Government should introduce a national campaign to educate adults on cybersecurity, based around the launch of the new National Reporting Hotline.

And yet, these measures are often not taken by adults, either. Our research found that people often do not change their cybersecurity habits - even after they have been scammed. We recommend that government should seek to capitalise on the unique opportunity afforded by the launch of the new National Reporting Hotline, to promote a new national campaign of cybersecurity awareness for their citizens

Beyond these seven measures, which are targeted at the US and UK together, but deserve international consideration, we have also identified three valuable country-specific recommendations.

Within the US, greater resources must be invested in the government's central cybersecurity coordination bodies:

Recommendation 8: The US government should strengthen the Cyber Infrastructure Security Agency (CISA), providing it with sufficient resources to coordinate private-public collaboration for combating cyber threats.

In contrast to the UK, where the central cybersecurity coordination body (the NCSC) is highly effective, the equivalent infrastructure is far less developed in the United States.[78] Specifically, CISA lacks the same ability to coordinate across government, and with the private sector, to share information and guidance about dealing with cyberthreats.

While much of CISA's focus is on larger cyberthreats, such as to infrastructure, improving the resources available to this body would do much to help resolve the issues posed by lower-level cybercrime and fraud. By building a more integrated and cooperative cybersecurity environment, a stronger CISA would facilitate greater opportunities for US government and law enforcement to collaborate with the private sector to tackle cybercrime.

Recommendation 9: The US government should introduce a post of National Cyber Director, responsible for enhancing the US' public-private work and international collaboration efforts.

In addition, we recommend the introduction of a National Cyber Director in the US, to facilitate collaboration around cybercrime: a measure that would provide similar benefits to strengthening CISA. While a Cyber Director would (again) primarily manage the response to high-level cyberthreats, a single figure responsible for cybersecurity collaboration would also yield substantial benefits for the US response to low-level cybercrime and cyber fraud. It is important to acknowledge this policy was also proposed by the Cyberspace Solarium Commission, suggesting that this is a well-regarded policy that the US government might adopt.[79]

This position would enhance collaboration with international partners, and help build closer cooperation between US government, law enforcement and key private sector stakeholders. Coupled with a strengthened and better-resourced CISA, these two measures would help transform the US into a far more 'mature partner for the private sector',[80] when trying to tackle cybersecurity issues.

Finally, we recommend one specific measure, within the UK, for ensuring it remains an effective international partner in countering cybercrime and fraud:

77. Interview, Mark Montgomery.
78. Interview, Mark Montgomery and Rob Morgus.
79. USA Cyberspace Solarium Commission. Cyberspace Solarium Commission. 2020. Available at https://www.solarium.gov/ [accessed 14/10/2020]
80. Interview, Rob Morgus.

Recommendation 10: The UK government should reach effective security and policing agreements with the EU, following Brexit, to ensure British police forces retain access to European intelligence and joint investigative work.

The UK has been a generally effective international partner in dealing with cybercrime and fraud, particularly via its contribution to the work done by Europol. But leaving the EU presents a severe threat to this effort, as it risks the UK losing access to the vital work done by this body and the substantive investigative material available in European databases.[81]

As a result, the UK government must ensure that close and effective security and policing agreements are reached with the EU, post-Brexit. Law enforcement efforts to tackle cybercrime inevitably require international collaboration, to help identify threats and gather the information required to investigate criminal organisations. Reaching agreements which provide access to databases and joint investigative work is vital to protect the UK's status as an effective international partner.

81. Sabbagh, D., Boffey, D, O'Carroll, L., Bowcott, O. and Inman, P. UK police 'unable to cope' if no-deal Brexit cuts EU data sharing. Available at https://www.theguardian.com/politics/2020/oct/20/uk-police-will-be-unable-to-cope-if-no-deal-brexit-cuts-eu-data-sharing [accessed 21/10/2020]

GLOSSARY

FORMS OF CYBERCRIME

Cyber-Dependent Crime - crimes which can only be committed via digital technologies, meaning that without these tools, they would not exist. An example of this is hacking, which cannot occur offline.

Cyber-Enabled Crime - crimes which could occur without the use of digital technologies, but are exacerbated by the use of these tools. An example of this is fraud, which increasingly occurs in online spaces, but can occur offline too.

Identity Theft - the theft of personal information or data which would allow the criminal to convincingly impersonate a victim, usually for financial gain - (e.g.) to obtain access to a bank account or to apply for a loan in their name.

Malware - malicious software deployed by cybercriminals and other actors in cyberspace, designed to damage a digital device, computer or any data held on such a device.

Phishing - malicious digital communications, designed to impersonate legitimate contacts such as banks, to trick targets into giving away personal information or data.

Ransomware - a specific form of malware, which locks a device and (usually) encrypts the data held on it. A ransom is then demanded from the user, to restore access to their data or device. This kind of malware is targeted at both individuals and larger organisations.

Romance Fraud/Scam - a specific form of fraud, in which criminals feign romantic interest in a victim, in order to exploit them into providing or sending money. This kind of fraud is particularly reliant on effective social engineering - see below.

Social Engineering - the 'human side' of a cybercrime, in which criminals identify, target and exploit the emotional vulnerabilities or psychological weaknesses of victims, to successfully defraud and manipulate them.

KEY ORGANISATIONS

International

Europol - the law enforcement agency run by the European Union (and its member states), responsible for sharing information between national law enforcement partners and conducting joint investigations into high-profile criminal activity.

UK

Action Fraud - the UK's national centre for the reporting of all fraud and cybercrime cases, via its phone number 0300 123 2040.

City of London Police - the lead police force for economic crime and fraud investigations in the UK.

Information Commissioner's Office (ICO) - a public body within the UK, responsible for protecting the privacy of individuals' data, with the ability to impose fines on private companies which lose the data of citizens.

National Crime Agency (NCA) - the UK's national-level law enforcement agency, which takes responsibility for combatting high-level, serious and organised criminality.

National Cyber Crime Unit (NCCU) - a unit housed within the National Crime Agency, responsible for leading and coordinating the national-level response to critical cyber incidents.

National Cyber Security Centre (NCSC) - the UK's central body responsible for leading collaboration around cybersecurity, including both cross-government and public-private collaboration.

National Fraud Intelligence Bureau (NFIB) - the UK's national body for assessing and evaluating any cases reported through Action Fraud, to determine whether they should be investigated in more detail.

Regional Organised Crime Units (ROCUs) - ten regional policing units, spread across England and Wales, which contain specialist capabilities - including some cybercrime expertise.

US

Cybersecurity and Infrastructure Security Agency (CISA) - the US central body, within the Department of Homeland Security, responsible for managing cybersecurity coordination at the national level.

Federal Bureau of Investigation (FBI) - the US' national-level law enforcement agency, which investigates federal crimes, and also functions as a domestic intelligence agency.

Internet Crime Complaint Center (IC3) - the US' national reporting hub for cybercrime and fraud cases, housed within the Federal Bureau of Investigation.

National Cybersecurity and Communications Integration Center (NCCIC) - a centre within CISA, which is responsible for sharing information with the private sector around cyberthreats.

National Cyber Investigative Joint Task Force (NCIJTF) - a task force housed within the FBI, integrating cyber expertise from law enforcement, defence and intelligence agencies, to provide expert investigation and analysis of cyber offences.

DEMOS

PUBLISHED BY DEMOS NOVEMBER 2020

15 WHITEHALL, LONDON, SW1A 2DD
T: 020 3878 3955
HELLO@DEMOS.CO.UK
WWW.DEMOS.CO.UK