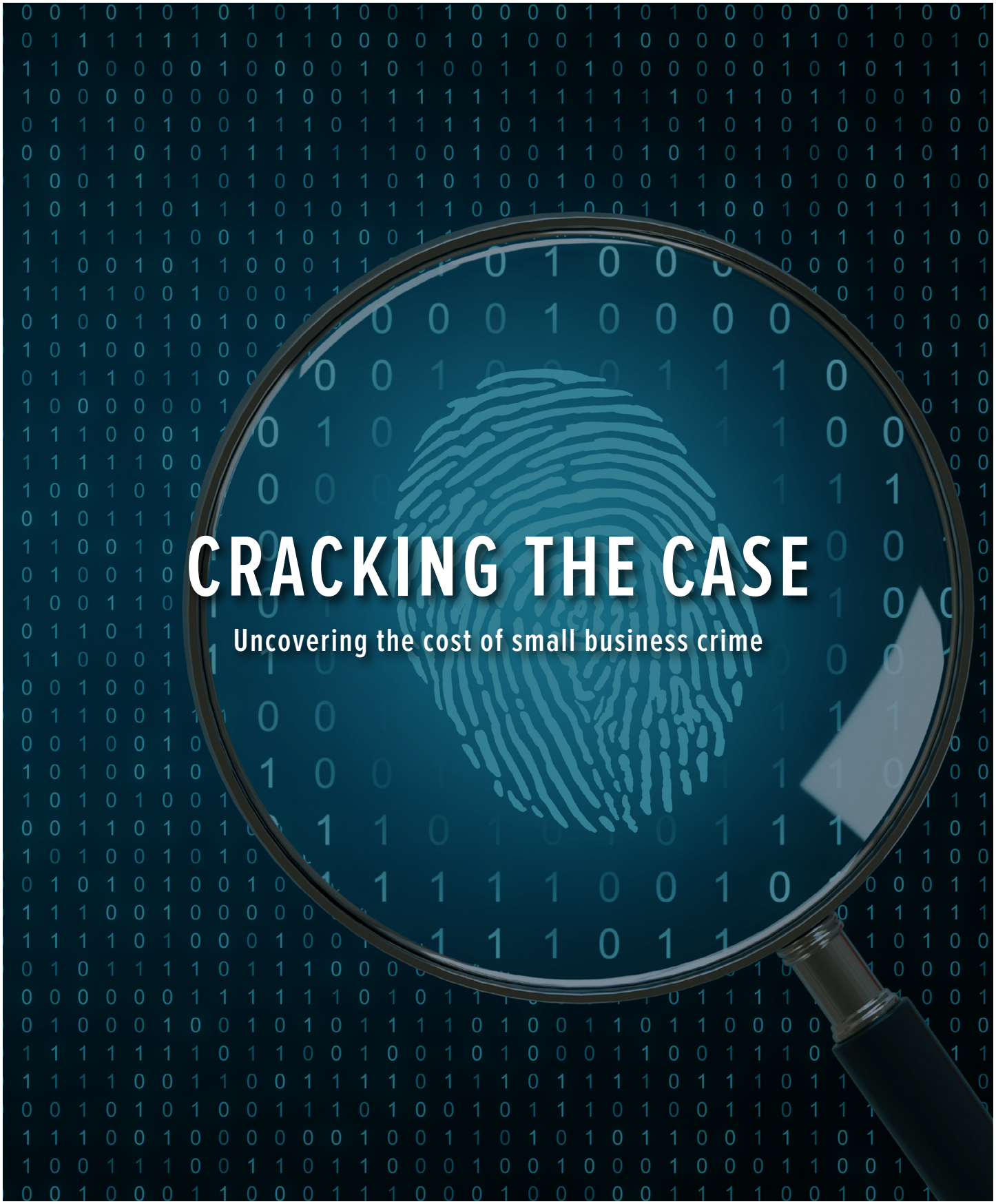


CRACKING THE CASE

Uncovering the cost of small business crime

Published: December 2023

@fsb_policy

fsb.org.uk

Federation of Small Businesses

ACKNOWLEDGEMENTS

This report was authored by Kristina Grinkina, Policy Advisor for business crime. Special thanks to FSB's policy, public affairs and media teams, in particular: Emelia Quist, Head of Policy Research, Tom Blenkinsop, Senior Public Affairs Advisor and Yupina Ng, Media and Communications Officer.

Thanks also to the following FSB colleagues: Kiera Marshall, Deputy Head of Policy (Wales); Dr Llŷr ap Gareth, Head of Policy (Wales); and Karen Woolley, Development Manager (Staffordshire and West Midlands).

This report would not have been possible without the FSB members across the UK who participated in this research, generously taking the time out of running their small businesses to complete our survey, attend focus groups and respond to interviews.

The quantitative research was carried out by Verve – the market research agency responsible for administering the survey. The report was designed by Cactus Design Limited – a small business based in Wales. This project would not have been possible without all the FSB members who participated in this research, generously taking the time out of running their small businesses.

WHO WE ARE

The Federation of Small Businesses (FSB) is the UK's grassroots business organisation. We are a cross-party non-profit body that represents small business and self-employed members in every nation and region.

For 50 years, we have been the authoritative voice on policy issues affecting the UK's 5.5 million small businesses, microbusinesses and the self-employed. FSB is the UK's largest business group and leading business campaigner, focused on achieving change which supports smaller businesses to grow and succeed.

We also provide our members with a wide range of vital business services, helping them to start, run, and grow successful businesses through high quality protection and support. This includes 24/7 legal support, financial expertise, training and events, debt recovery and employment/HR advice – alongside a powerful voice heard by governments at all levels.

Our local, national and international activism helps shape policy decisions that have a direct impact on the day-to-day running of smaller businesses. We work for their interests through research and engagement with our members and by effective campaigning - influencing those in power through policy analysis, public affairs, media and public relations activity.

Our policy and advocacy work starts with our expert team in Westminster, which focuses on UK and England policy issues, the UK Government, Parliament and the media. Further to this, our teams in Glasgow, Cardiff and Belfast work with governments, elected representatives and media in Scotland, Wales and Northern Ireland.

CRACKING THE CASE

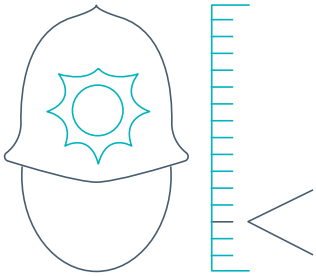
Uncovering the cost of small business crime

11%

of small businesses in England and Wales say **traditional crime, such as vandalism** has **cost them more than £10,000** in the last two years

81%

of small businesses in England and Wales have **experienced at least one type of business crime** in the last two years



20%

of small businesses that did not report a crime cited **lack of confidence in the police / Action Fraud** as one of the reasons

72%

of small businesses have **experienced cybercrime** in the last two years

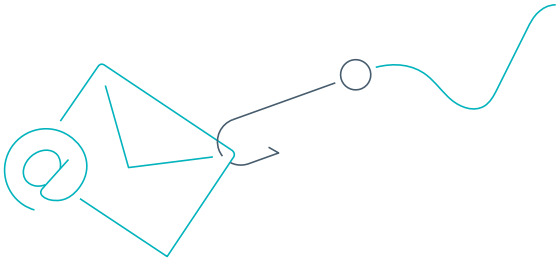
56%

of small businesses say they have **invested more in cybersecurity and anti-fraud measures** in the last two years

An estimated

1.89m

small businesses say that they have **experienced fraud** in the last two years



92%

of the most **frequently reported types of cybercrime is phishing**

26%

of small businesses say they have experienced **unauthorised payments from bank cards/accounts**

CONTENTS

FOREWORD

Small business crime is often overlooked – it doesn't make headline news or Parliamentary debates. As such year after year, election after election, small business crime is forgotten. In 2019, FSB published Calling Time on Business Crime[1], the report highlighted the corrosive impact of business crime on small businesses across England and Wales.

FSB research shockingly and conclusively shows a rise in threatening behaviour, intimidation, and or assault over the last four years, alongside increased reports of serious organised shop theft. This problem needs swift attention if we are to protect and support vulnerable small businesses and those who work in them. The publication of the Government's Anti-Social Behaviour Action Plan is welcome to help focus resources; however, more could still be done at a local level to protect small firms in their communities.

Fraud is now the most common crime in the UK, costing almost £7 billion a year. Worryingly, incidents of small business cybercrime have more than tripled, highlighting the ineffectiveness of measures taken against business crime to date. Small firms find themselves abandoned and increasingly exposed. Fraud accounts for 41 per cent of offences in England and Wales, with only 1 per cent of police resources dedicated to it.[2] There needs to be a greater focus on the impact of fraud on small businesses and a commitment to support smaller businesses to tackle it, as it can not only be life changing for the business owner but have a negative impact on the local economy.

Small businesses are not complacent; they are taking measures to protect themselves. However, given the severity of the damage and fallout from crime that they suffer this is not enough, and more action should be taken by government, law enforcement and wider industry to help tackle business crime. The difficulties around reporting and calculating the impact of crime can also lead to resources being misdirected. Infrastructure must be put in place to enable forces to classify business crime.

Greater collaboration between forces and support from national leads is needed. Data from Action Fraud also needs to inform the allocation of police resources locally and nationally, and greater responsibility should be placed on online services through requiring implementation of greater security measures.

Small businesses are affected by crime, directly financially and indirectly through wider social and reputational impacts. Criminal acts against small businesses act as a barrier to their growth and innovation. Small business crime is not a victimless crime. It impacts business owners, staff, and local communities and ultimately local and national economic growth.

Neil Sharpley
Policy Champion, Regulation, Crime, Online, and Dispute resolution

1 FSB report, Calling time on business crime: Safeguarding small firms for the future, 2019, https://www.fsb.org.uk/resource-report/calling-time-on-business-crime.html
2 Committee of Public Accounts, Progress Combatting Fraud, 2023 https://publications.parliament.uk/pa/cm5803/cmselect/cmpubacc/40/report.html

EXECUTIVE SUMMARY

This report covers crimes experienced by small firms from January 2021 to January 2023, some of this period overlapped with coronavirus pandemic and government instructions to limit social contact. Coronavirus restrictions led to fewer incidents of crimes such as theft and robbery, which is reflected in our research.

The report includes insights gathered through in-depth survey work and qualitative evidence collected from interviews with small businesses in England and Wales.

This report covers three types of crime:

- Traditional crime refers to traditional, physical-world crimes such as theft, burglary, arson etc.
- Cybercrime refers to criminal acts that involve causing damage to computer systems, internet-enabled devices, or the information held on those devices, or gaining unauthorised access to online accounts such as banking, email or social media etc.
- Fraud refers to the use of trickery or deception in order to gain personal or financial information.

Traditional crime

Traditional crime has continued to affect the small business community. Crimes such as anti-social behaviour, burglary and theft have continued to plague the lives of small business owners. Small businesses that suffer from traditional crime are more likely to report a financial impact than from other types of crime, with majority costs attributed to fixing damage to property and replacing stock. To aid prosecution and tackle organised crime a single online portal should be introduced which would allow business complainants and other victims to submit witness statements and simple evidence such as CCTV images directly to the police. This would enable cost savings in terms of police resources as well as help to identify organised and prolific offenders.

Cybercrime and fraud

The disruption that small businesses face considering rising cybercrime and sophistication of fraud incidents continues to be a challenge. From the persistence of phishing emails, which many small businesses have been affected by over the last two years to almost a third that have experienced invoice fraud. Small businesses and self-employed entrepreneurs typically have more limited time and resources than their larger counterparts, which increases the risk of inability to detect exposure to criminals operating online.

However, small businesses are not complacent. Our evidence shows that more than half of small businesses have increased their investment in cybersecurity and anti-fraud measures over the last two years. Despite this, small firms should not carry the burden of cybercrime defence alone. The government should require online services such as online platforms, social media platforms and e-mail providers that hold personal and financial information to enhance their security measures by, for example, introducing multi-factor authentication to prevent the hacking of online accounts.

Policing and reporting crimes

Small businesses that have experienced traditional crime are more than twice as likely to report crime to the police than those who have experienced fraud or cybercrime. For those that do not report crime, the most common reasons for not reporting a crime include it not being serious enough to report and a lack of confidence in the police.

Introducing a mandatory recording process for business crime similar to that of assault and burglary will improve crime data in England and Wales. This will help to drive better outcomes for businesses and the police through more efficient and targeted resource allocation.

KEY FINDINGS

Prevalence of crime in England and Wales from January 2021 to January 2023

- 81 per cent of small businesses have experienced at least one crime.
- 35 per cent of small businesses have experienced at least one 'traditional' business crime such as theft, burglary, arson etc.
- 37 per cent of small businesses have experienced fraud.
- 72 per cent of small businesses have experienced cybercrime.

Small business experience of business crime

Of those smaller businesses that experienced at least one traditional crime, the most frequently reported crimes are:

- Vandalism/damage to premises, anti-social behaviour (34%)
- Burglary or robbery (30%)
- Theft by a third/external party (29%).

Of those smaller businesses experienced at least one fraud, the most frequently reported types are:

- Invoice fraud (31%)
- Card/cheque fraud (29%)
- Unauthorised payments from bank cards/accounts (26%).

Of those smaller businesses that experienced at least one cybercrime, the most frequently reported cybercrimes are:

- Phishing (92%)
- Malware attack (10%)
- Social media hacked (9%).

Financial cost of crime

89 per cent of small businesses in England and Wales that have experienced traditional crime say that they have faced a financial cost. Of those small businesses that experienced traditional crime:

- 33 per cent say that it cost up to £1,000
- 56 per cent say that it cost more than £1,000, and
- 11 per cent say that it cost more than £10,000.

83 per cent of small businesses say that they have experienced a financial cost following the most impactful fraud. Of those small businesses that experienced fraud:

- 44 per cent say that it cost up to £1,000
- 39 per cent say that it cost more than £1,000, and
- 8 per cent of small businesses say that it cost more than £10,000.

73 per cent of small businesses say that they have experienced a financial cost following the most impactful cybercrime. Of those small businesses that experienced cybercrime:

- 44 per cent say that it cost up to £1,000
- 30 per cent say that the financial cost was more than £1,000, and
- 6 per cent of small businesses say that it cost more than £10,000.

Wider impacts of crime

Of those small businesses who have suffered any type of crime from January 2021 to January 2023, 72 per cent report wider impacts. These include:

- Having to purchase replacement equipment, fixtures and fittings (13%)
- Lost stock (11%)
- Payment providers charging back cost of fraud to their business (10%)
- Negative impact on businesses reputation (10%)
- Delayed delivery of products/services to customers (9%)
- Increased insurance premiums and/or excesses (6%).

Measures that businesses take to protect themselves from crime

65 per cent of small businesses in England and Wales report taking at least one measure to protect themselves from traditional crime. These include:

- Installing or upgrading security (including CCTV) (37%)
- Initiating a training programme (16%)
- Improved insurance cover (12%).

92 per cent of small businesses report taking at least one measure to protect themselves from cybercrime and fraud. These include:

- Have anti-virus software on devices (83%)
- Regularly update software on IT systems (74%)
- Regularly back up data and IT systems and test them (55%)
- Insurance protection (20%).

Policing and reporting crimes

66 per cent of small businesses in England and Wales say that they have reported their most impactful crime. Of those smaller businesses:

- 30 per cent reported it to the police
- 20 per cent reported it to their bank
- 18 per cent reported it to their IT provider/service.

31 per cent of small businesses did not report their most impactful crime in the last two years. The most frequently reported reasons for not reporting crime are:

- Not serious enough to report (43%)
- Lack of confidence in the police/Action Fraud (20%)
- No plans to make an insurance claim (15%)
- Takes too long (7%)
- Too difficult to report (5%).

Of those smaller businesses that reported their most impactful crime from January 2021 to January 2023:

- 59 per cent state the police did not attend the scene
- 39 per cent say they received a crime number, but the police did not attend
- 5 per cent say an officer came within an hour
- 4 per cent say an officer arrived within 24 hours
- 48 per cent say the police did not investigate after the initial police response
- 3 per cent say the police investigated, identified and arrested the perpetrators.

RECOMMENDATIONS

Traditional crime

Police and Crime Commissioners should:

- Include business crime as a priority in their Police and Crime Plans and in manifestos for all those standing for election in May 2024 demonstrating commitments to business crime from the beginning to the end of their term (p.27).
- Establish a business crime board which would include representatives from range of businesses to help share insights and intelligence and the impact of crime as well as contribute to better decision making and targeting of resources (p.27).

Home Office should:

- Introduce a separate offence for violence against retail workers (p.27).
- Clarify that there is no £200 threshold for investigating organised shoplifting offences. There is currently an impression that shoplifters will not be arrested if they steal under £200 worth of goods. Correcting this impression would send a clear message that lower value organised shoplifting offences will not be tolerated (p.28).

Home Office should work with the Ministry of Justice to:

- Introduce a single online portal which would allow for more efficient prosecution and action from law enforcement in relation to minor offences such as theft where prosecution rates are too low (p.27).

Local authorities should:

- Be supported to recruit and retain Neighbourhood Wardens to complement the work of the police in relation to anti-social behaviour (ASB) (p.28).

Department for Environment, Food & Rural Affairs (Defra) should:

- Work with local authorities to set a clear national framework for tackling fly-tipping, setting overall expectations and promoting good practice, while allowing local authorities the flexibility to respond to local circumstances (p.28).

Small businesses should:

- Familiarise themselves with the ICO's guidance on CCTV[3] to ensure they're compliant with data protection rules (p.28).

3 Information Commissioner's Office, CCTV checklist https://ico.org.uk/for-organisations/advice-for-small-organisations/checklists/data-protection-self-assessment/cctv-checklist/

Cybercrime and fraud

UK Government should:

- Establish a cross-departmental committee on tackling fraud and cybercrime. The cross-departmental committee would allow for more intelligence sharing across departments to better foresee any challenges for example, on coordination on any associated risks and suggestions for suitable mitigation (p.41).
- Publish guidance and advice on cyber and fraud protection together with any schemes that they promote to small businesses on the use of software or other products that put them at risk of cybercrime or fraud (p.41).
- Publish guidance for any third-party providers that provide Cyber Essentials scheme compliance to businesses to encourage them to be transparent on essential and non-essential costs in attaining the certification (p.41).
- Publish appropriate guidance and consider information campaigns aimed at small businesses to help them identify enforcement agents to ensure that they are legitimate and help to promote these through Cyber Resilience Centres (p.41).

UK Government and National Cyber Security Centre should:

- Review the pricing of Cyber Essentials certification as well as costs associated with annual renewal in relation to the smallest businesses and explore whether lower tier pricing or a special reduced rate could be introduced (p.41-42).

Home Office should:

- Include the impact of fraud on small businesses in the next fraud strategy and consider a specific targeted approach with clear objectives to tackling it (p.42).
- Make unauthorised data copying a separate offence under the Computer Misuse Act (p.42).

Department for Science, Innovation and Technology should:

- Require large online services such as online platforms, social media platforms or e-mail providers to implement greater security such as multi-factor authentication to help prevent the hacking of online accounts and take action to close fake accounts on social media platforms (p.42).

Policing

Home Office should:

- Introduce a mandatory recording process for business crime and add a 'business crime' section to the crime outcomes in England and Wales statistics so progress can be tracked, and targets set (p.52).
- Aim to increase the average number of police officers in England and Wales up to 335 per 100,000 population to help dedicate appropriate resources for crime against businesses including cybercrime and fraud (p.52).
- Use the data collected by new Action Fraud reporting system, which is due to be launched in 2024, when allocating resources nationally between forces and encourage the same within police forces (p.52).

National Police Chiefs' Council should:

- Cut red tape for police forces, to allow them to focus on solving crime. The National Police Chiefs' Council found that 443,000 officer hours are spent filling in unnecessary forms and burdensome administrative tasks (p.53).[4]
- Commit to attending the scene of incidents of traditional business crime where there has been an aggravating factor such as violence or damage to premises, and progress should be tracked and reported for accountability (p.53).

4 Home Office, Police given more time to focus on solving crimes and protecting public, 2023 https://www.gov.uk/government/news/police-given-more-time-to-focus-on-solving-crimes-and-protecting-public

EXPERIENCE OF CRIME BY SMALL BUSINESSES IN ENGLAND AND WALES

Business crime is a broad and ever-evolving problem. Small firms experience all types of crime from vandalism, serious acquisitive crime, cybercrime and fraud. The prevalence of crime to small businesses has increased since the publication of FSB's, 2019, *Calling Time on Business Crime* report.[5]

Eighty-one per cent small businesses in England and Wales have experienced at least one type of business crime in the last two years. Over a third (35%) of small businesses say they have experienced at least one traditional crime in England and Wales in the last two years, and this more than doubles to 72 per cent of small businesses who have been targeted by cybercriminals.

While the number of small businesses reporting experiencing traditional crime has remained largely unchanged since 2019 (34%), the number of small businesses reporting to have experienced cybercrime has more than tripled from 20 per cent in 2019 to 72 per cent in 2023.

Interestingly, when comparing incidence of cybercrime across nations, small businesses in Scotland are less likely to say they have experienced cybercrime, either attempted or successful, committed against them (64%) than those in England and Wales. Over a third (37%) of small businesses report being targeted by fraudsters in the last two years.

Figure 1: Types of crime experienced by small businesses in England and Wales
Source: FSB business crime survey, 2023

Type of crime	At least one business crime
Traditional	35%
Fraud	37%
Cybercrime	72%

The data becomes even more staggering when comparing this with the business population statistics to illustrate the true scale of crime on smaller business. The Government estimates that there were in total 5,127,495 SMEs in England and Wales in 2023, meaning that according to FSB research an estimated 1.79 million small businesses experienced (either attempted or successful) traditional crime, 1.89 million fraud and 3.69 million cybercrime.[6]

5 FSB report, Calling time on business crime: Safeguarding small firms for the future, 2019, https://www.fsb.org.uk/resource-report/calling-time-on-business-crime.html
6 Department for Business and Trade, Business population estimates 2023 https://www.gov.uk/government/statistics/business-population-estimates-2023

Figure 2: Estimated number of SMEs that suffered from different types of crime in England and Wales

Source: FSB business crime survey, 2023

Type of crime	Number of businesses
Traditional	1.79 million
Fraud	1.89 million
Cybercrime	3.69 million

Experience of crime also varies according to size of the business. Small businesses with employees (78%) are more likely to say that they have suffered from at least one type of business crime than those who are self-employed (22%). There are a variety of reasons why small businesses with employees are more likely to be at risk of crime.

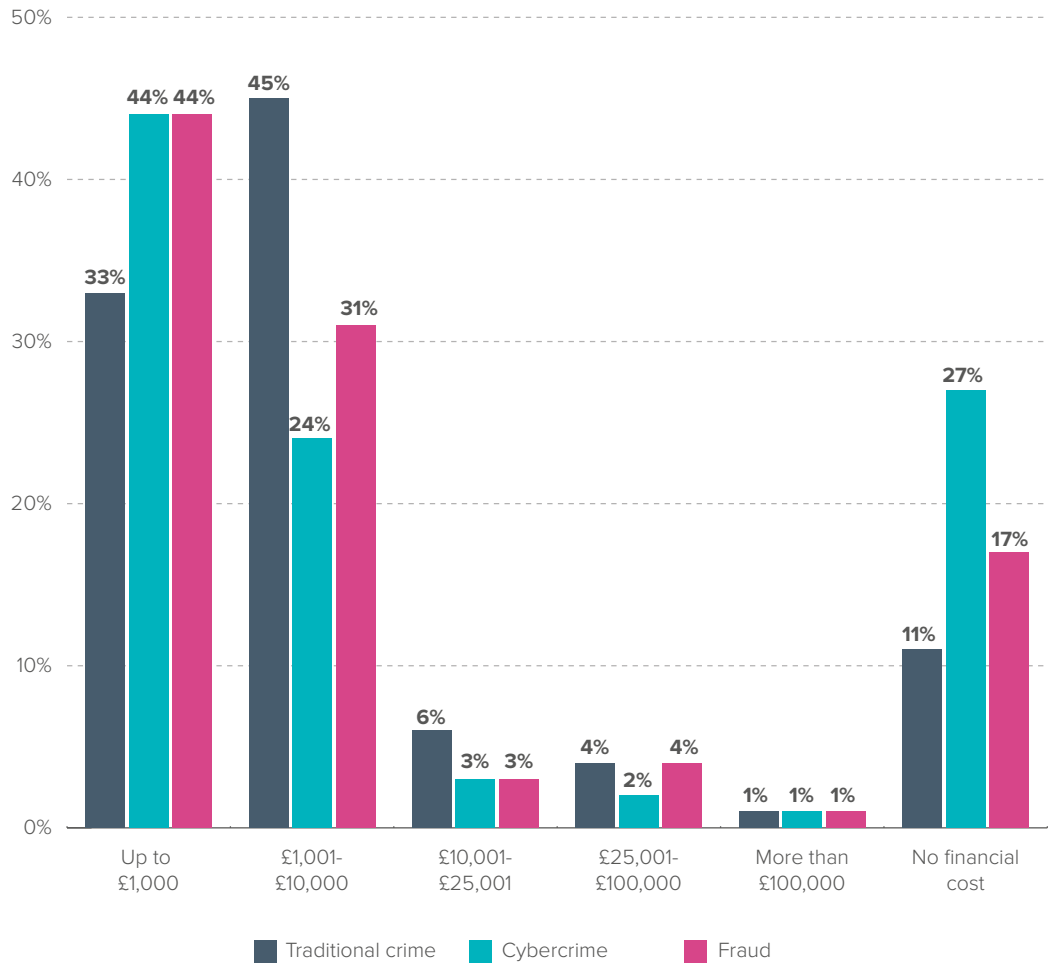
The impact of crime on small businesses

The impact of crime on small businesses is substantial. 89 per cent of small businesses that have been victims of traditional crime say they have suffered a financial impact and 83 per cent of small businesses say they have suffered a financial impact after being a victim of fraud in the last two years. Small businesses who have experienced cybercrime are slightly less likely to say that they have suffered a financial impact (73%) in comparison to the other two types of crime.

This could be because that cybercrime is more likely to be visible when the attack has been unsuccessful and therefore, while businesses may experience an attempt it does not have a financial impact on the business. Nevertheless, across all types of crime majority of small businesses say have suffered a financial impact in the last two years.

Figure 3: Financial impact of crime on small businesses in England and Wales in the last two years

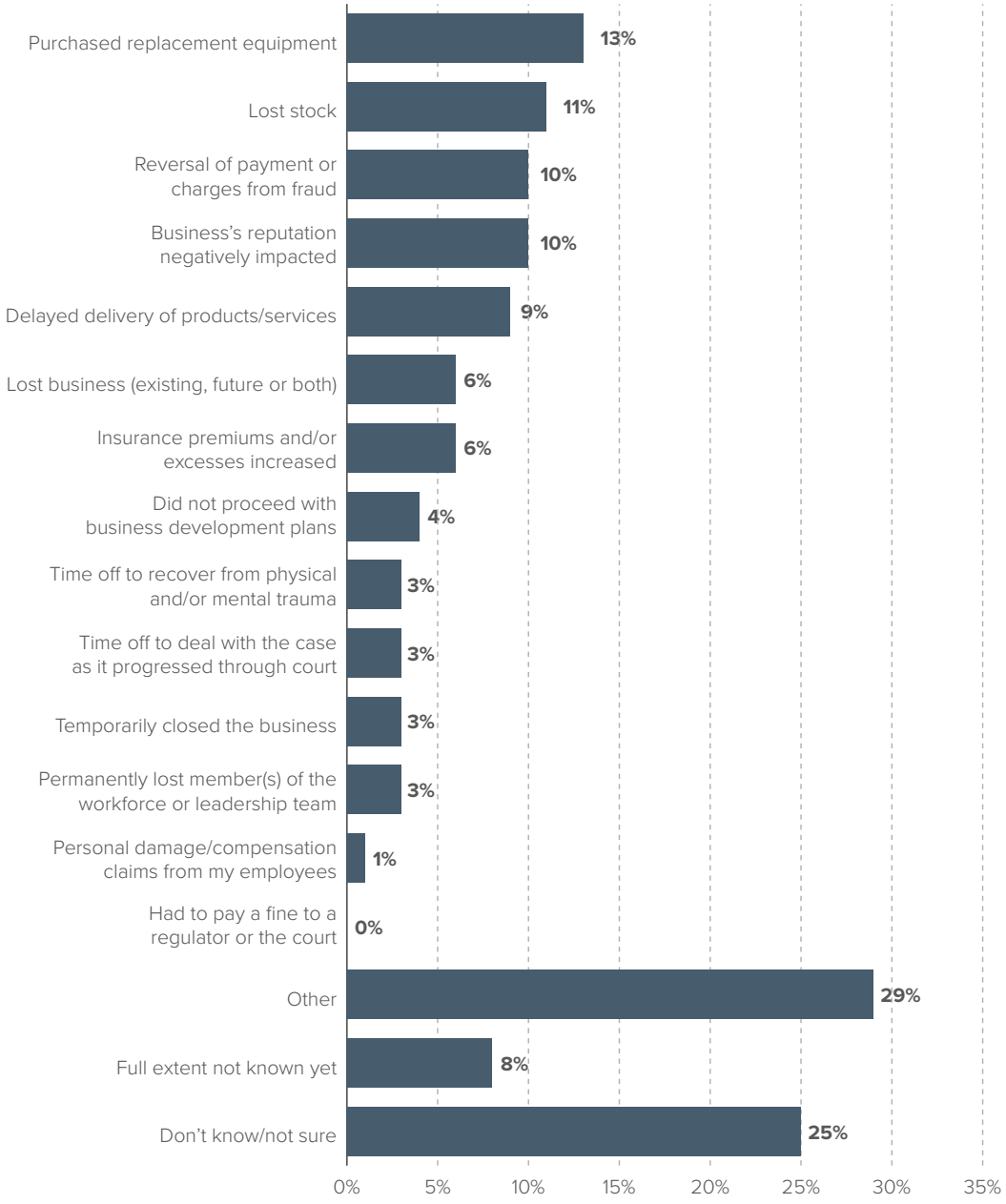
Source: FSB business crime survey, 2023



Of those who have experienced any type of crime, 72 per cent reported wider impacts of crime on their business. Most frequently reported impacts are having to purchase replacement equipment, fixtures and fittings (13%), lost stock (11%), payment providers charging back cost of fraud to their business and business reputation negatively impacted (both 10%).

Figure 4: Wider impacts of crime on small businesses in England and Wales

Source: FSB business crime survey, 2023



“We’re an online retailer, and often experience credit card fraud. Our big problem is that the buck stops with us. So, if there is a potential fraudulent transaction, it’s a.) up to us to work that out and b.) there’s nobody to check if it is fraudulent or not. There’s nothing to tell us if a card is fraudulent or not, and it’d be useful if we could speak to a bank and verify information. What happens is we either end up losing a sale because we’ve decided this is fraudulent, and perhaps it isn’t, or we end up sending out goods, and we then have to refund payments, and then we get penalised. This leads to extra charges by the credit card companies, it seems rather unfair.”

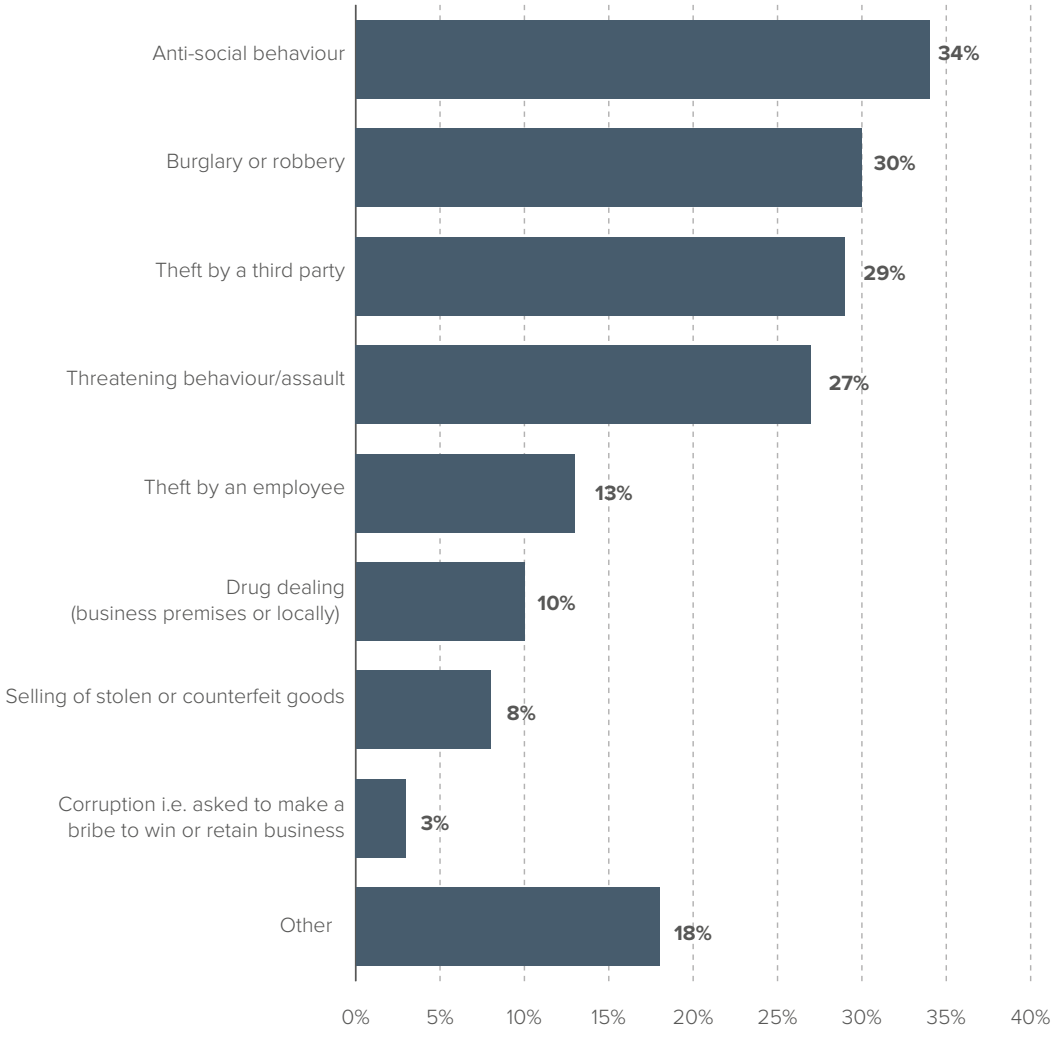
FSB member, online retail business, South West England

TRADITIONAL CRIME

Over a third (35%) or an estimated 1.79 million small businesses in England and Wales say that they have experienced at least one traditional crime in the last two years. Examples of traditional crime include burglary or robbery, theft by a third party, anti-social behaviour and using the business premises or local area for dealing of drugs.

The most frequently reported crimes are vandalism/damage to premises and/or anti-social behaviour (34%), burglary or robbery (30%) and theft by a third/external party (29%).

Figure 5: Types of traditional crime experienced by small firms in England and Wales
Source: FSB business crime survey, 2023



GEOGRAPHICAL DISTRIBUTION OF TRADITIONAL CRIME

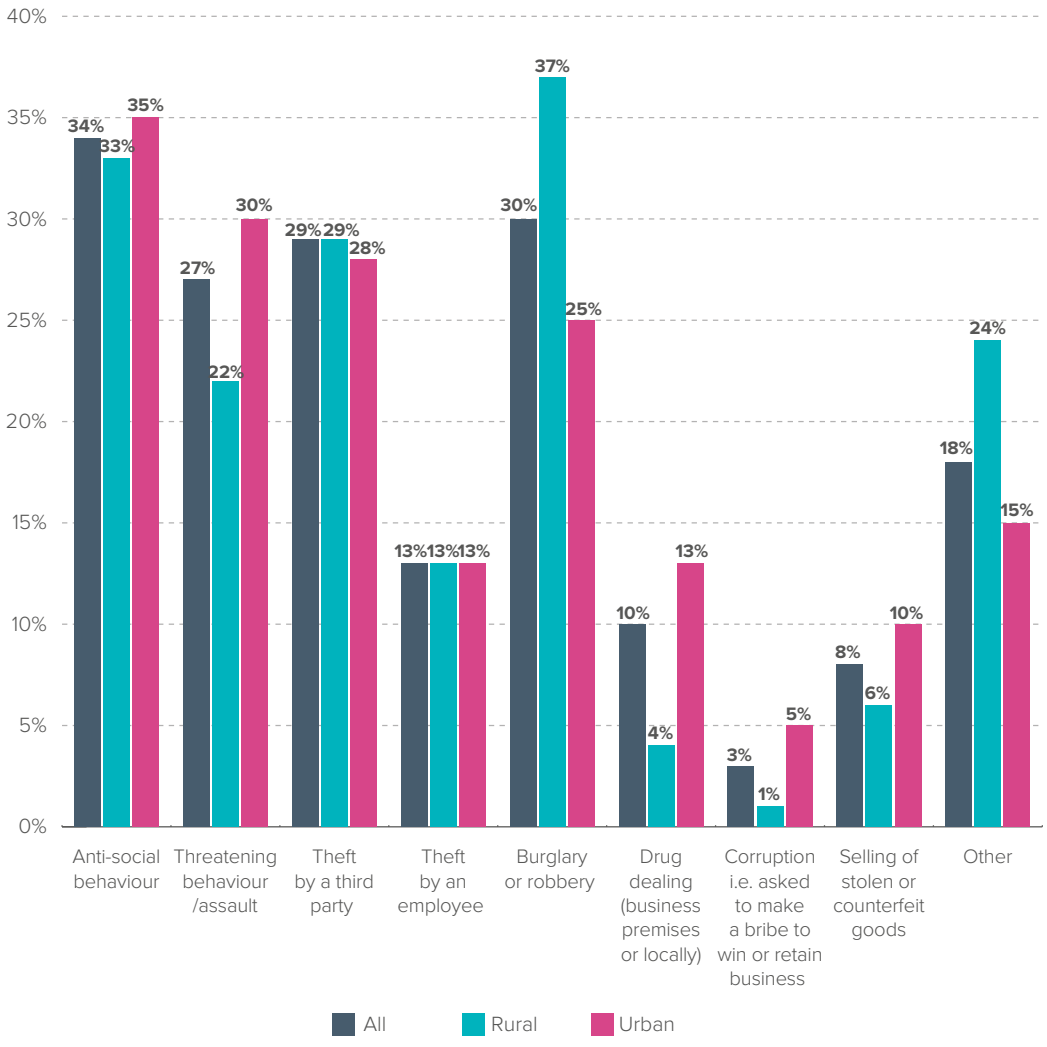
Small business crime differs across cities, towns, villages and rural areas. Rural crimes such as thefts of agricultural machinery have a significant impact on rural communities and businesses. FSB research shows differences in the rates of types of traditional crime for rural and urban based small businesses in England and Wales (Figure 6).

"I work from home, so, I'm always a bit more cautious, because my business premises is an office from home, so I've got CCTV cameras installed, partly to do with the business with quite a rural location but partly because of safety."

FSB member, Land development and planning business, East of England

Figure 6: Types of traditional crime experienced in rural and urban areas by small firms in England and Wales

Source: FSB business crime survey, 2023



House of Commons Library research briefing published in September 2023, stated 'in rural areas, the loss of branches may easily result in much longer journeys and where digital alternatives are hampered by poor internet connectivity. And closure is likely to have more serious effects when the last branch of any bank in a community disappears'.[7] Our research shows of those small businesses that have experienced traditional crime in rural areas are more likely to have experienced burglary or robbery (12%) than small firms in urban areas (9%). FSB members in rural areas have consistently raised bank closures and the challenges this presents locally; travelling further to deposit cash exposes small business owners in rural areas to undue risks.

FSB members also raised concerns about waste crime in rural areas, a crime which often goes unreported, and has consequential costs for businesses including having to dedicate resources for clear up. The Department for Environment, Food & Rural Affairs (Defra) published the Resources and Waste Strategy in December 2018, the strategy committed to several actions including a Joint Unit for Waste Crime and toughening penalties for waste criminals.[8] However, progress on such policies has been slow.

The 2022 Public Accounts Committee report stated, 'Defra does not have an outline delivery plan for achieving its ambition of eliminating waste crime by 2043.'[9] Like many areas of crime, the lack of data is holding back effective solutions and the delivery of justice. Local authorities could do more to report fly tipping to the Agency and Defra should provide more support to local authorities especially in rural areas where this is a growing problem.

Small businesses with employees

Small businesses with no employees are more likely to say that they have not experienced traditional crime (81%) than businesses with employees, (one to nine employees (63%) and 10-49 employees (45%).

In August 2022, an aggravated factor offence was added to assaults, including those of shopworkers, meaning that those who are violent towards working in retail will receive harsher punishments.[10] However, at the time of writing it is unclear whether any prosecutions have been successful. The situation is complicated further as the Home Office does not track the offence. There have also been calls to make violence against retail workers a separate criminal offence in order to give victims the protection that they deserve. FSB support this recommendation.

7 Steve Browning, Research Briefing: The future of local banking services and access to cash, 2023 https://commonslibrary.parliament.uk/research-briefings/cbp-9453/

8 Department for Environment, Food & Rural Affairs and Environment Agency, Resources and waste strategy for England, 2018 https://www.gov.uk/government/publications/resources-and-waste-strategy-for-england

9 Committee of Public Accounts, Government approach to large parts of waste crime "closer to decriminalisation" than tackling it, 2022 https://committees.parliament.uk/committee/127/public-accounts-committee/news/173604/government-approach-to-large-parts-of-waste-crime-closer-to-decriminalisation-than-tackling-it/

10 Stuart Anderson MP, Question for Attorney General, Emergency Services and Retail Trade: Crimes of Violence, 2022 https://questions-statements.parliament.uk/written-questions/detail/2022-06-27/26004/

Counterfeit goods

An increasing number of smaller businesses report experiencing crimes related to the sale of counterfeit goods. Counterfeit goods undercut and undermine legitimate businesses, pose risks to consumer safety, reduces income tax and funds and allows other criminality to flourish.

In recent years, many small firms have moved online in response to changes in consumer behaviour. Online trade extends opportunity for availability of counterfeit goods to a wider market, and consequentially increases the risk to small firms of greater exposure to this type of crime.

Anti-social behaviour

Of those small businesses in England and Wales that experienced traditional crime, 34 per cent say that they have experienced vandalism, damage to premises and/or anti-social behaviour. Vandalism and anti-social behaviour can be particularly damaging to smaller businesses and can consequentially reduce local economic growth and negatively impact the wellbeing of local residents.

In March 2023, the Government published the Anti-Social Behaviour Action Plan, a welcome move in addressing anti-social behaviour (ASB) in England and Wales. In particular the announcement of the launch of a digital tool to report anti-social behaviour, funding for Police and Crime Commissioners (PCCs) working with councils to target enforcement and the introduction of hot spot policing to target ASB areas are positive changes.[11] Hot spot policing is particularly effective at targeting anti-social behaviour in high problem areas.[12] Similarly, a recent National Business Crime Survey of businesses regarding anti-social behaviour found that over half (55%) of businesses report a desire to see an increased police presence to help tackle ASB.[13]

Neighbourhood policing is key in tackling ASB. Effectively utilising Neighbourhood Warden programmes and ensuring councils are able to attract and retain them, for example through allocating appropriate funding adjusted according to the level of anti-social behaviour in an area could also be effective particularly where better reporting and data is needed of its incidence. Similarly, delivery of Bystander Training Programme's locally could also be beneficial for those challenging behaviours and supporting witnesses. While recent announcements in hot spot policing are a step in the right direction in helping to tackle anti-social behaviour, we believe that the Government could go further in increasing police and local authority presence in target areas.

11 Department for Levelling UP, Housing & Communities and Home Office, Anti-Social Behaviour Action Plan, 2023 https://www.gov.uk/government/publications/anti-social-behaviour-action-plan/anti-social-behaviour-action-plan

12 College of Policing, Targeting approaches to crime and disorder reduction, 2021 https://www.college.police.uk/research/what-works-policing-reduce-crime/targeted-approaches

13 National Business Crime Centre, Anti-Social Behaviour Survey Report Released, 2023 https://nbcc.police.uk/index.php/news/anti-social-behaviour-survey-report-released

The fear of crime can have a real impact on personal well-being and social connections.[14] Previous FSB research on the ability of small businesses in creating social value in their communities found 80 per cent of small firms contributed to and/or volunteered with a local community organisation.[15]

Theft

Twenty-nine per cent of small businesses in England and Wales say they have experienced theft by a third party in the last two years.

> **"There is a huge amount of shoplifting (in the built environment sector). I feel it's seen as an acceptable business cost, so it's generally not prosecuted. There are massive repeat offenders who are tolerated. It might be a fine for them (perpetrators) but, it's not fine for you if you're a small operator. I feel there is massive amounts of organised crime, and organised shoplifting which goes back into funding other types of crime and criminal activity."**
>
> FSB member, Business consulting, South East England

In August 2023, the-then Home Secretary, Rt Hon Suella Braverman wrote to letter to encourage police to follow up on all reasonable lines of enquiry for all crime types including shoplifting and for no crime investigations being screened out as minor.[16] This was followed by the publication of the Retail Crime Action Plan which provided further detail on reasonable lines of enquiry, police attendance and the scene and advice on how to provide best possible evidence for retailers.[17]

Commitments to Project Pegasus have also been promising in relation to submitting CCTV or other digital images of perpetrators through Police National Database using facial recognition to identify prolific offenders.[18] However, there are concerns around the availability of relevant technology and systems for small businesses, meaning that many larger stores could be potentially steps ahead from small businesses and the unintended consequences could be that it pushes organised shoplifters towards the smaller stores where such technology may not be used.

14 ONS, Chapter 3: Personal well-being and crime, 2015 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/compendium/crimestatisticsfocusonpublicperceptionsofcrimeandthepoliceanddthepersonalwellbeingofvictims/2015-03-26/chapter3personalwellbeingandcrime

15 FSB report, Small Business, Big Heart: Bringing Communities Together, 2019 https://www.fsb.org.uk/resource-report/small-business-big-heart-communities-report.html

16 Home Office, Pursuing all reasonable lines of enquiry: letter to police leaders, 2023 https://www.gov.uk/government/publications/pursuing-all-reasonable-lines-of-enquiry-letter-to-police-leaders/pursuing-all-reasonable-lines-of-enquiry-letter-to-police-leaders

17 National Business Crime Centre, New Retail Crime Action Plan published, 2023 https://nbcc.police.uk/news/new-retail-crime-action-plan-published

18 Home Office, Action plan to tackle shoplifting launches, 2023 https://www.gov.uk/government/news/action-plan-to-tackle-shoplifting-launched

Cost and impact of traditional crime

One of the key concerns raised by small businesses is a perception that theft is considered an acceptable business cost. However, this should not be the case, especially for small and micro businesses. Of those small businesses that have experienced at least one type of traditional crime, 89 per cent suffered a financial impact from their most impactful crime. More than half (56%) of small businesses say their most impactful traditional crime cost them £1,000 or more and more than one in ten (11%) say their most impactful traditional crime cost them more than £10,000 in the last two years.

Figure 7: Cost of the most impactful traditional crime experienced by a small business in the last two years in England and Wales

Source: FSB business crime survey, 2023

Estimated cost of traditional crime	Percentage of small businesses reporting
Up to £1,000	33%
£1,001 - £10,000	45%
£10,001 - £25,000	6%
£25,001 - £100,001	4%
More than £100,000	1%
No financial cost	11%

Of those that have suffered a financial impact from traditional crime, around a fifth (21%) say the majority of costs fell on fixing damage to property and 19 per cent say costs fell on replacing stock.

The cost of lost business time is also a significant factor for small businesses in dealing with the impacts of crime. 14 per cent of small businesses say the majority of costs of dealing with traditional crime went on covering the cost of lost business time including dealing with police and insurance. The impacts of traditional crime have been widely reported, for example the Government's Commercial Victimisation Survey highlighted similar impacts of financial loss as well as loss of goods, services and additional staff time spent on dealing with the fallout of crime.[19]

Crime has a long-lasting impact. The top impacts reported by small businesses include negative impact on wellbeing (34%), decline in business revenue (28%) and insurance premiums and/or excesses increased (27%).

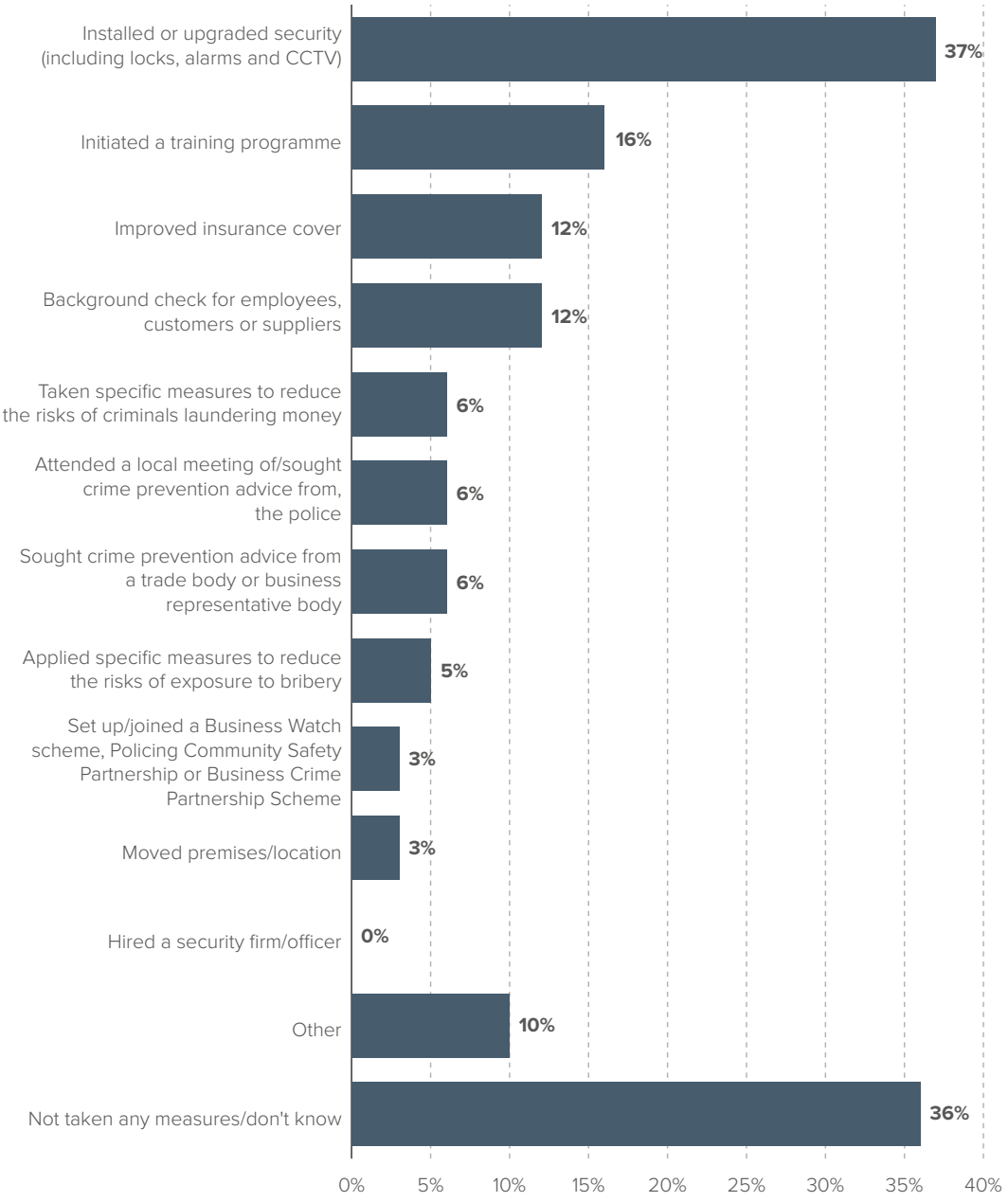
19 Home Office, Crime against businesses: findings from the 2022 Commercial Victimisation Survey, 2023 https://www.gov.uk/government/statistics/crime-against-businesses-findings-from-the-2022-commercial-victimisation-survey

Prevention of traditional business crime

Over two thirds (65%) of small businesses in England and Wales report taking at least one step to protect themselves against traditional crime. The most frequently reported measures small firms state they have taken include installing or upgrading security (including locks, alarms and CCTV) (37%), initiating a training programme (16%), improving insurance cover (12%), and background checks for employees (12%).

Figure 8: Types of defensive measures that businesses take to protect themselves from traditional crime in England and Wales

Source: FSB business crime survey, 2023



CCTV can be an effective tool for deterring crime particularly when taken together with other crime prevention measures.[20] However, small businesses have also reported issues with the use of CCTV particularly in rural locations and difficulties about the ability to use CCTV as evidence. Interestingly, our research shows small firms in rural areas (43%) are more likely to have installed or upgraded security and CCTV than small firms in urban areas (33%).

"We're a rural business which comes with additional challenges; if you have a contract for CCTV monitoring connectivity is an issue. Our broadband is just not fit for purpose. It does not work at all."

FSB Member, Consultancy, East of England

In addition, new smart CCTV technology which may use facial recognition technology is expensive for many small firms.

"We have CCTV equipment installed inside and outside of our premises. Someone opened a vehicle with an electronic device which turned the alarm off, they took around £8,000 worth of equipment. We had clear CCTV footage of the vehicle and the people involved. We gave this information to the police, but the response was, unless you've got clear picture of the person's face there's nothing we can do."

FSB member, Manufacturing and construction business, North West England

20 Eric L. Piza et al. CCTV surveillance for crime prevention: A 40 year systematic review with meta analysis, 2019 https://www.researchgate.net/publication/331981674_CCTV_surveillance_for_crime_prevention_A_40-year_systematic_review_with_meta-analysis

Recommendations

Police and Crime Commissioners should:

- **Include business crime as a priority in their Police and Crime Plans and in manifestos for all those standing for election in May 2024 demonstrating commitments to business crime from the beginning to the end of their term.** In 2022, 93 per cent of PCCs Police and Crime Plans featured business crime as a priority.[21] This is welcome and should continue to be encouraged so that business crime is a priority for all PCCs. This should become a fundamental part of every PCC's plan from the beginning. In addition, a steer from the Home Secretary to Chief Constables on business crime could affirm that this is a priority.
- **Establish a business crime board which would include representatives from range of businesses to help share insights and intelligence and the impact of crime as well as contribute to better decision making and targeting of resources.** This is already established by some PCCs and should be adopted more widely. The board should include business representatives that reflect the business population locally including small businesses to help ensure a diversity of views.

Home Office should work with the Ministry of Justice to:

- **Introduce a single online portal which would allow for more efficient prosecution and action from law enforcement in relation to minor offences such as theft where prosecution rates are too low.** The single online portal would allow business complainants and other victims to submit witness statements and simple evidence such as CCTV images directly to the police online, allowing for swift action to be taken in relation to perpetrators. This would also enable tackling organised crime offenders and improve data collection with regard to crime prevention and could also be linked with existing proposals and developments with the Pegasus project which would lead to a more efficient prosecution and evidence collation process.

Home Office should:

- **Introduce a separate offence for violence against retail workers.** The Retail Crime Action Plan commits to attending the scene where violence has been used against shopworkers, and the work on the Pegasus project has been a step in the right direction. However, it is unclear that the introduction of the aggravated factor in shoplifting last year has been effective as Home Office does not track the offence. It could therefore be beneficial to introduce a separate standalone offence to protect victims and ensure that this is seen to be on the same footing as other violent offences.

21 Association of Police and Crime Commissioners, National Lead supports Business Crime Week of Action, 2022 https://www.apccs.police.uk/latest-news/national-lead-supports-business-crime-week-of-action/

- **Clarify that there is no £200 threshold for investigating organised shoplifting offences.** There is currently an impression that shoplifters will not be arrested if they steal under £200 worth of goods, which also feeds into the assumption that organised offenders stealing smaller amounts will not be prosecuted. Correcting this impression would send a clear message that lower value organised shoplifting offences will not be tolerated, which should have a deterrent effect on organised shoplifters and build trust among small businesses who fall victim to this crime. The commitments in the Retail Crime Action Plan are promising, however anecdotal evidence suggests that businesses do not believe that organised crime offences will be investigated appropriately.

Local authorities should:

- **Be supported to recruit and retain Neighbourhood Wardens to complement the work of the police in relation to anti-social behaviour (ASB).** Local authorities do have some limited powers in tackling crime, and should be enabled and supported with resources to complement the work of the police, in tackling anti-social behaviour for example, through on the spot fines and providing vital intelligence and reporting of incidents. The additional data from exercise of such powers would better inform the government's hot spotting initiative helping to increase the number of police officers with the numbers of prolific offenders in an area, which would in turn help to better enforce and repair damage done to local businesses.

Department for Environment, Food & Rural Affairs (Defra) should:

- **Work with local authorities to set a clear national framework for tackling fly-tipping, setting overall expectations and promoting good practice, while allowing local authorities the flexibility to respond to local circumstances.** Defra could do more to support local authorities to tackle fly-tipping, particularly where local authorities are constrained by limited resources. Where funding has been allocated previously this has been awarded on the basis of bidding, favouring local authorities with larger capacities leading to different approaches and abilities of authorities to deal with these issues.

Small businesses should:

- **Familiarise themselves with the ICO's guidance on CCTV[22] to ensure they're compliant with data protection rules.** Out of small businesses that take at least one measure to protect themselves from traditional crime, over a third (37%) report installing or upgrading security including CCTV. Given that data protection law covers the use of CCTV, small businesses should familiarise themselves with the relevant guidance on installing and operating systems so that they comply with the rules.

22 Information Commissioner's Office, CCTV checklist https://ico.org.uk/for-organisations/advice-for-small-organisations/checklists/data-protection-self-assessment/cctv-checklist/

CYBERCRIME AND FRAUD

Cybercrime

The Covid-19 pandemic accelerated small business adoption of digital technologies. Digital presence became a widespread necessity because of the need to engage with customers, however, this swift reaction also exposed a number of small firms to threats which they had previously not considered or been exposed to. The Office for National Statistics (ONS) estimates that fraud and computer misuse offences increased substantially between March 2020 and March 2022 with computer misuse increasing by a total of 89 per cent in that a period and fraud by 25 per cent.[23]

"We had a ransomware attack a few years ago and we were saved from that because we have backups elsewhere, through which we were able to recover the data; because I managed to recover nearly all of our data we didn't have to pay out."

FSB member, Acoustic consultancy, East of England

Our research shows there has been an exponential growth in cybercrime and fraud. Over two thirds (72%) or an estimated 3.69 million small businesses say that they have experienced cybercrime in the last two years. Given that cybercrime refers to criminal acts that are online enabled, it is not surprising that it is largely indiscriminate of business size.

Phishing attacks are the most common method identified by businesses in the government's Cyber Breaches Survey 2023[24] and the National Cyber Security Centre's Active Cyber Defence research which reflects FSB research.[25] Of the 72 per cent of small businesses that have experienced cybercrime in the last two years, more than nine in ten (92%) say that they have been targeted through phishing emails.

"Every member of staff gets a weekly email targeted to one of the areas of cybersecurity...we're cyber essentials accredited. If we detect a weak link because of a member of staff, then we address this issue with them and educate them."

FSB member, IT management business, East Midlands

Phishing is a form of social engineering whereby targeted messages through texts or e-mails, or calls are made that use deception to encourage a user to make an action such as click on a link, document or make a call which then may be used to steal personal data or financial details. These are particularly cunning in the current climate where there are increasing cost pressures and users may be more tempted by deals, discounts or rebates. Some financial institutions as well as larger online platforms have notably started to

23 ONS, Nature of fraud and computer misuse in England and Wales: year ending March 2022 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022

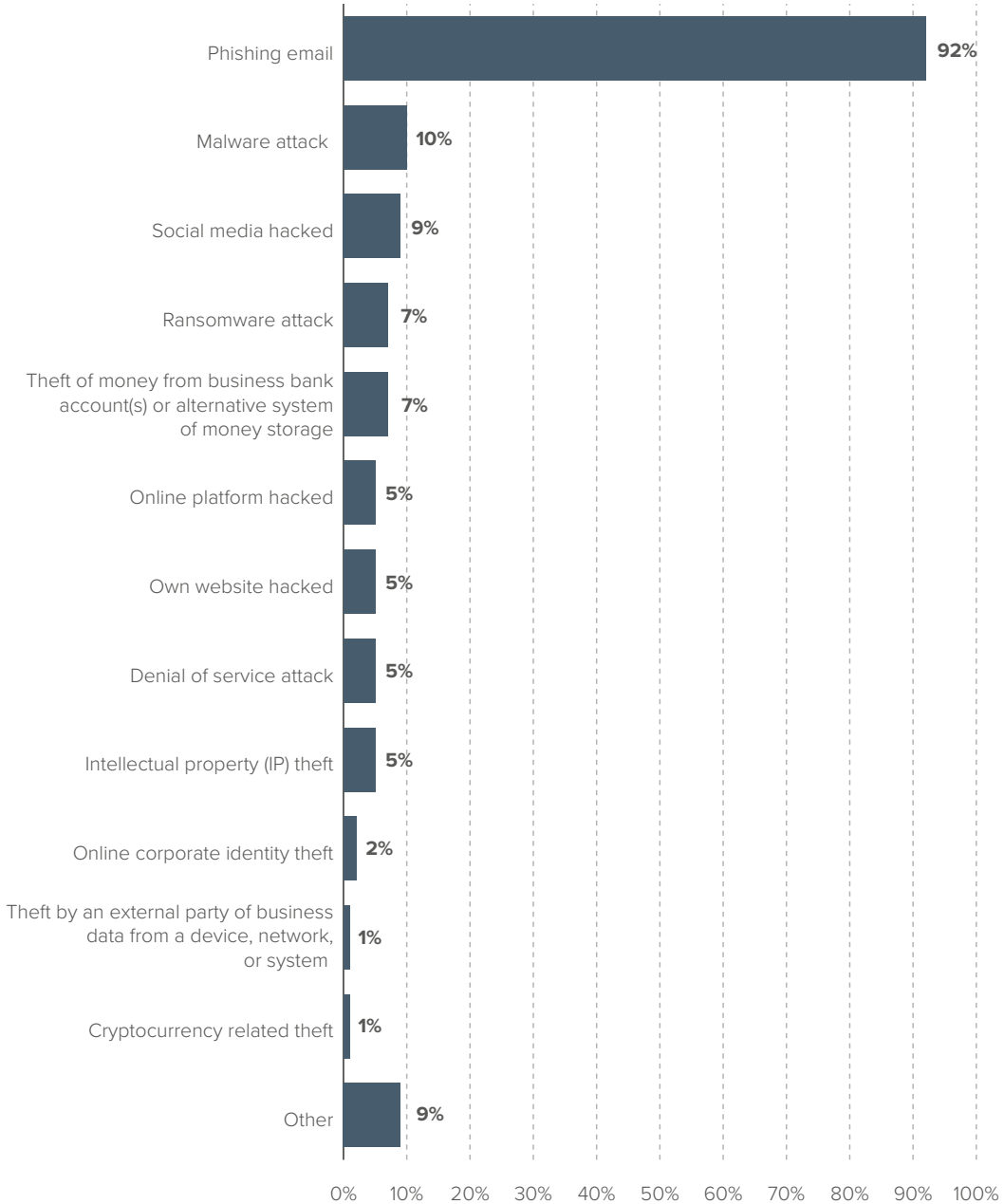
24 DSIT, Cyber security breaches survey 2023 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023

25 NCSC, Support from British businesses crucial in removing over 235,000 scams, new figures reveal, 2023 https://www.ncsc.gov.uk/news/british-business-support-crucial-in-removing-scams

move risk away from the user by removing direct links from their communications to their customers and instead providing instructions to access information through an app or their website.

Figure 9: Types of cybercrime attempted or committed against small businesses in the last two years

Source: FSB business crime survey, 2023



There are sectoral differences in the experience of cybercrime. Small businesses in manufacturing and wholesale and retail sectors (both 77%) are more likely to say they have experienced cybercrime than those in the professional, scientific and technical activities sector (71%).

Small business experiences of cybercrime also vary, from failed attempts to successful attacks that have had a severe and lasting impact on the business.

"I regularly get people sending me emails. You know the old, here's an invoice you need to pay just click here. So far, to my knowledge, the only successful activity was to get through to the back end of my website and sticking one of these scam pages on and also had begun to email out of my website. Now I thought I was pretty well locked down and I've no idea how they managed to get into the back end of the website. My provider couldn't tell me how they got in either and the only way I could get rid of it and be sure was completely destroy the website."

FSB member, Business consultancy, South East England

Fraud

References to cybercrime and fraud profiles are frequently interchangeable due to fraud often being cyber-enabled. A report from the House of Commons Committee of Public Accounts, *Progress combatting fraud* found fraud accounts for 41 per cent of crimes committed in England and Wales, and that 81 per cent of all fraud offences in the UK are now cyber enabled.[26] Fraud can also be committed by letter, telephone or in-person, and the perpetrators can include employees acting internally, or external attacks by criminal opportunists posing as customers.

"We issue all our invoices electronically. We create PDFs of those invoices, and then we then just email them to our clients. We got a phone call one day from one of our clients saying, "have you changed your bank details recently". We said no, and they said, "well, we've received an invoice from you with different bank details to your usual one and we've had a phone call from somebody asking us to pay immediately". It turns out somebody had intercepted our email and they had doctored the PDF, changed the bank details and then forwarded it to the clients, and then said, give us the money."

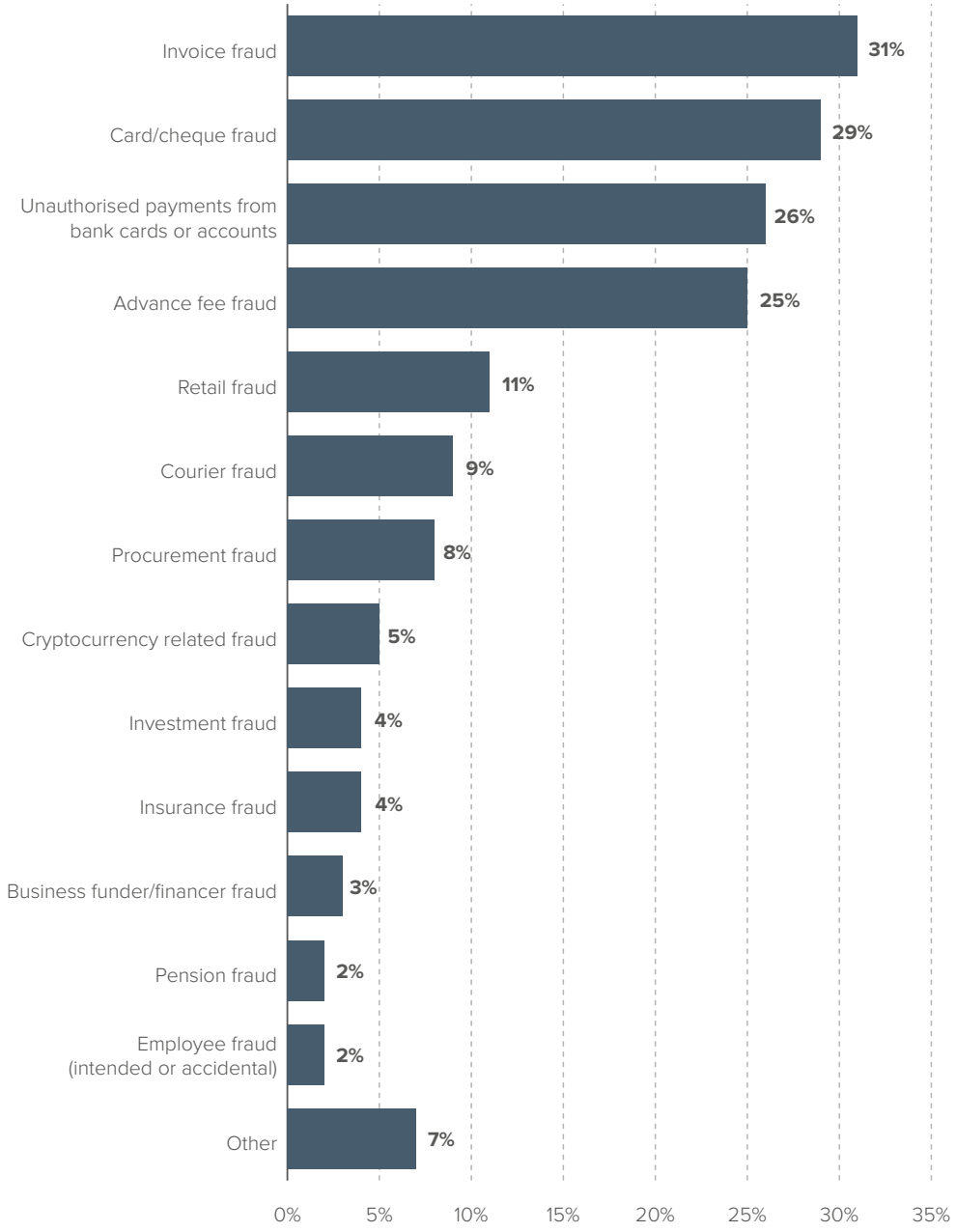
FSB member, Acoustic consultancy business, East Midlands

Over a third (37%) or estimated 1.89 million of small businesses say that they have fraud attempted or committed against them in the last two years. Of those small businesses, the most common types include invoice fraud (31%), card/cheque fraud (29%) and unauthorised payments from bank cards or accounts (26%).

26 Committee of Public Accounts, Progress combatting fraud, 2023 https://committees.parliament.uk/publications/34609/documents/190751/default/

Figure 10: Types of fraud attempted or committed against small businesses over the last two years

Source: FSB business crime survey, 2023



Fraud is often sophisticated and relies on putting pressure on the victim to make a payment or accessing personal details and accounts. One of the key concerns in relation to fraud is its evolving nature and sophistication for example, increased artificial intelligence (AI) usage is likely to exacerbate the problem in the future.

"I was victim of a fairly unpleasant bank fraud, which I actually knew nothing about until my bank called me. The villains emptied everything other than £10 out of a bank account, taking around £30,000. The deception was incredibly simple, but incredibly clever. They called my bank, claiming to be me, and said, they wished to make a transfer in spite of the fact I had instructed my bank that I wanted to opt out of telephone banking.

The bank asked for my security codes, but the fraudsters didn't know this information, so the bank called me on my mobile number. However, the fraudster had already contacted my mobile provider and had diverted my calls to them. So, the fraudster was able to reset my security codes and emptied my bank account.

I reported it to Action Fraud, but I felt Action Fraud was disinterested. I got the money back, but it's such a clever scheme and I could do nothing to stop it because I was a totally unaware."

FSB member, Manufacturing, South East England

Rise of cybercrime and fraud has not been matched by the level of resources thus creating a permissive culture across the Government and law enforcement agencies. The delay in appropriate action to tackle scams from Government and law enforcement agencies has to some extent led to inertia from internet service providers, telecoms companies and the like. FSB supports the introduction of the National Fraud Strategy published in Spring 2023[27] outlining the commitment to launch a cross government anti-fraud public awareness campaign on how to avoid and respond to fraud and scams. The sophistication of fraud will require businesses to keep pace with any new developments so information campaigns can be helpful. Government guidance and actions must also keep pace, especially as use of AI tools by criminals likely to continue to increase that sophistication.

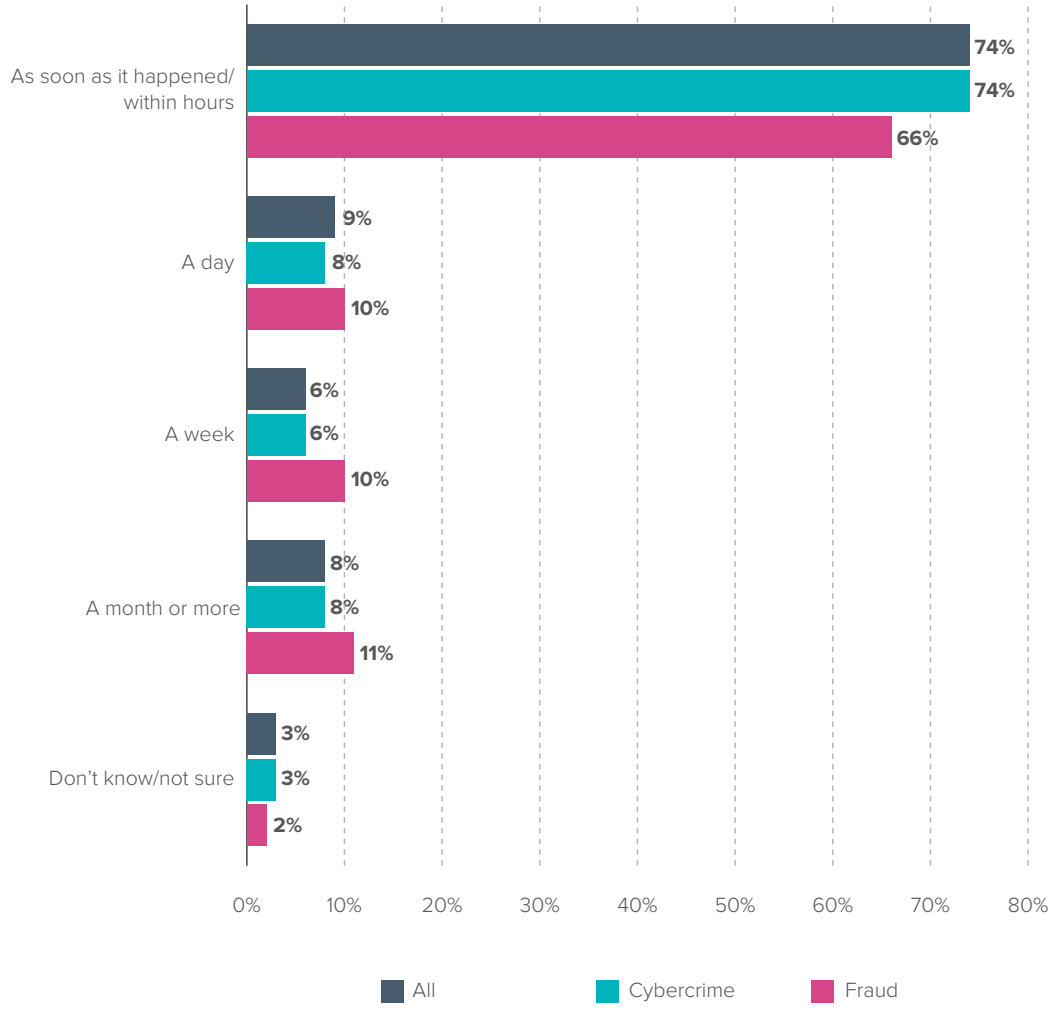
Another big part of defence and mitigation of fraud and its impact is being able to recognise risk as soon as possible and prevent it escalating to cause extensive damage and/or losses. Almost three quarters of small businesses (74%) say they detected a cybercrime had been attempted or committed as soon as it happened or within hours, this drops to two thirds (66%) for those who detected that a fraud had been attempted or committed within the same timeframe. Cybercrime and fraud can often go undetected for longer periods of time in comparison to crimes such as theft or vandalism which are more likely to be immediately recognised by the victim, this in turn can make them more difficult to recover losses and catch perpetrators.

27 Home Office, Fraud Strategy: stopping scams and protecting the public, 2023 https://www.gov.uk/government/publications/fraud-strategy

> **"I've had incidents where my company's bank account details have been used to set up direct debit insurance covers for five supercars. I only became aware when I started getting letters from insurers, who thankfully had recognised that it was highly improbable that this was the company that the insurance should have been placed against. The direct debits had actually been set up on my bank account, but fortunately no payments had been made."**
>
> FSB member, Consultancy business, South East

Figure 11: Length of time it takes to detect that cybercrime or fraud has been attempted or committed against a small business

Source: FSB business crime survey, 2023



"I was out of the country and my financial controller received a request from my email address asking her to transfer €36,000 to a potential purchase company account. We didn't go through with the transfer. Those kinds of attempts are extremely cunning."

FSB member, Research and development company, East Midlands

Cost and impact of cybercrime and fraud

Economic crime costs the UK economy at least £290 billion per year.[28] The financial cost of cybercrime and fraud can have a substantial impact on a small business. Small businesses which experience fraud are more likely to say that they have suffered a financial cost following an incident (83%) than those who had experienced cybercrime (73%).

Of the small businesses that have experienced a financial cost (both from cybercrime and fraud) 43 per cent say that it has cost them £1,000 or less in the last two years. 39 per cent of small businesses say that fraud has cost them more than £1,000 in the last two years, this drops to 30 per cent to those who say the same for cybercrime.

Figure 12: Cost of most impactful cybercrime or fraud to small businesses

Source: FSB business crime survey, 2023

	All (cybercrime and fraud)	Cybercrime	Fraud
Up to £1,000	43%	44%	44%
£1,001- £10,000	24%	24%	31%
£10,001-£25,000	3%	3%	3%
£25,001 - £100,000	2%	2%	4%
Over £100,000	1%	1%	1%
No financial cost	27%	27%	17%

Of those that have suffered a financial impact from cybercrime and fraud, just under a third (30%) say the majority of the costs fell on either installing or researching additional cyber security software (including antivirus), and 12 per cent say that the majority of the costs went on covering the cost of lost business time, i.e. time spent dealing with police, insurance claims, ICO etc).

It is clear that if these types of crimes persist and increase in frequency, the impacts would be even more substantial for business owners and their businesses. The most common reported possible future impacts include a negative impact on their wellbeing (29%), decline

28 House of Commons debate, Economic Crime: Law Enforcement, 2022 https://hansard.parliament.uk/commons/2022-07-07/debates/D08E9A46-5BA8-4DA8-8E29-025C312722AE/EconomicCrimeLawEnforcement

in business revenue (22%) and delay in delivery of products or services (19%) and loss of existing and/or future business (16%).

Small businesses in our research have cited psychological impact as well as concerns about privacy following experiencing some types of fraud.

"I received a suspicious phone call from a company claiming to be a bailiff, saying that they were around the corner, and they were coming to collect goods to cover a debt of £5,000. It turns out it was a fraud. I didn't give them any money. I was extremely scared. I contacted the police and Action Fraud. The police weren't interested in doing anything because nothing had happened. Action Fraud didn't do anything either. I gave them telephone numbers, email addresses, contact details, transcripts of everything that had happened, and nothing came of it. My business is in my house, so I was concerned they would come and help themselves to anything."

FSB member, Lighting consultant, East Midlands

It is estimated that cybercrime amounts to 41 per cent of crime committed in the UK, but it is only given one per cent of the anti-crime budget. Considering the financial impact on small firms this suggests it is currently under-resourced.[29]

Prevention of cybercrime and fraud

Given the exposure of small businesses to the risk of cybercrime and fraud, and the severe consequences that can be associated with successful attacks and scams, it is critical for businesses to be able to protect themselves. 93 per cent of small businesses in England and Wales have taken at least one measure to protect themselves from cybercrime or fraud. This is similar to 92 per cent of small firms who say the same in Scotland.

The most common preventative measures include purchasing anti-virus software (84%), regularly updating software on IT systems (75%) and backing up data and IT systems and testing them (56%).

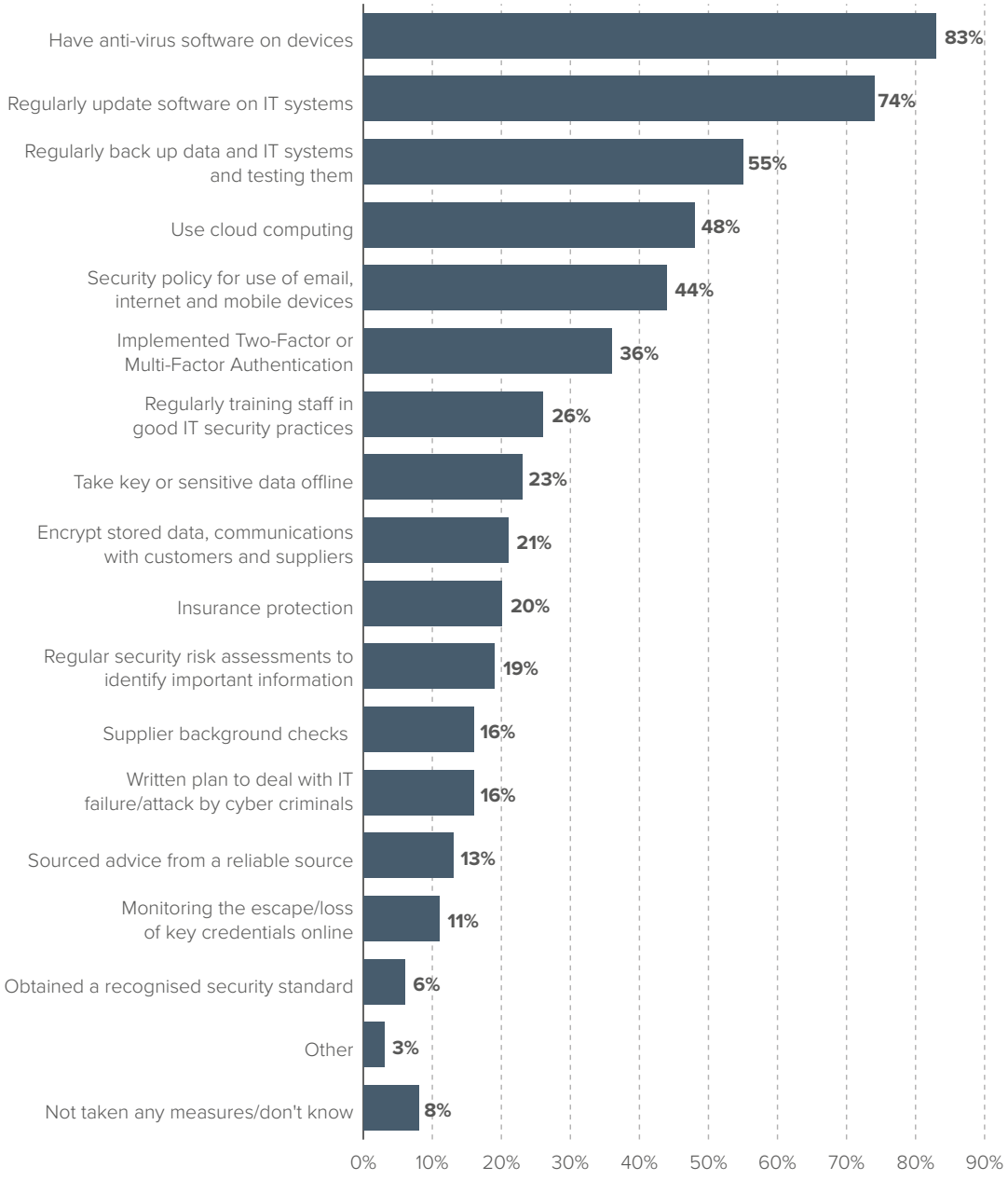
"We've not been victims of cybercrime, but we do receive daily phishing emails. We use office 365 and there is a method through that to report it."

FSB member, IT management company, East of England

29 House of Lords debate, Fighting Fraud (Fraud Act 2006 and Digital Fraud Committee Report), 2023 https://hansard.parliament.uk/Lords/2023-06-30/debates/AE4A7262-1126-4BED-8797-DB3853567E71/FightingFraud(FraudAct2006AndDigitalFraudCommitteeReport)

Figure 13: Types of defensive measures that businesses take to protect themselves from cybercrime and fraud in England and Wales

Source: Business crime survey, 2023



"If you understand the threat to your business, then you can go on to accurately assess the risk and conduct a risk assessment around all of your assets. That's data, paper and physical. A good risk assessment should be repeatable, and it should be done often. But you've got to understand the threat in order to do an accurate risk assessment. The outcome of the risk assessment will enable you to do the right thing, and that to do the right thing will look different, depending on what sort of business you're in. An agricultural business is going to be a lot different to a technical business. But it may be that the threat actors, the types of threat, the types of challenge that each business faces will be different."

FSB member, Cybersecurity company, East Midlands

Only six per cent of small businesses report obtaining a recognised cyber security standard (this could include ISO 27001 and Cyber Essentials); this has tripled from 2 per cent in 2019.[30] While this is an increase, the uptake is still relatively low, however, this is not surprising given the costs that are often associated with it.

The Government's evaluation of the Cyber Essentials scheme undertaken in June 2023 found that small and micro businesses often find that the certification is too expensive to renew and maintain, with micro business employers being quoted almost £2,000 annually to renew the certification.[31] The paper suggests a need to reform the pricing structure including review of the assessment fees and potentially introducing special rates for the smallest businesses at annual renewal. FSB support this recommendation.

On the other hand, small businesses also report concerns that some IT companies attempt to exploit the Cyber Essentials scheme and use it as a springboard to sell additional software in order to profit.

"We provide Cyber Essential Standards for Cyber Essentials Plus to small law firms in Wales, and we discovered that the [company's] relationship with their IT providers was absolutely awful. So many of them were just trying to sell products rather than to fix things. So, we saw organisations that had a free Cyber Essentials assessment that we provided, and then they were being told that they had to put made-up things in place. Things like you need to upgrade your firewalls, and you need to have a brand-new server. We had one client say that we can't do the free assessment because it's going to cost £7,000 to put everything right. We looked at what they said, and it was all made up. It was all fake."

FSB member, Cybersecurity company, Wales

30 FSB report, Calling time on business crime, 2019 https://www.fsb.org.uk/resource-report/calling-time-on-business-crime.html

31 Department for Science, Innovation & Technology, Cyber Essential scheme process evaluation, 2023 https://www.gov.uk/government/publications/cyber-essentials-scheme-process-evaluation/cyber-essentials-scheme-process-evaluation

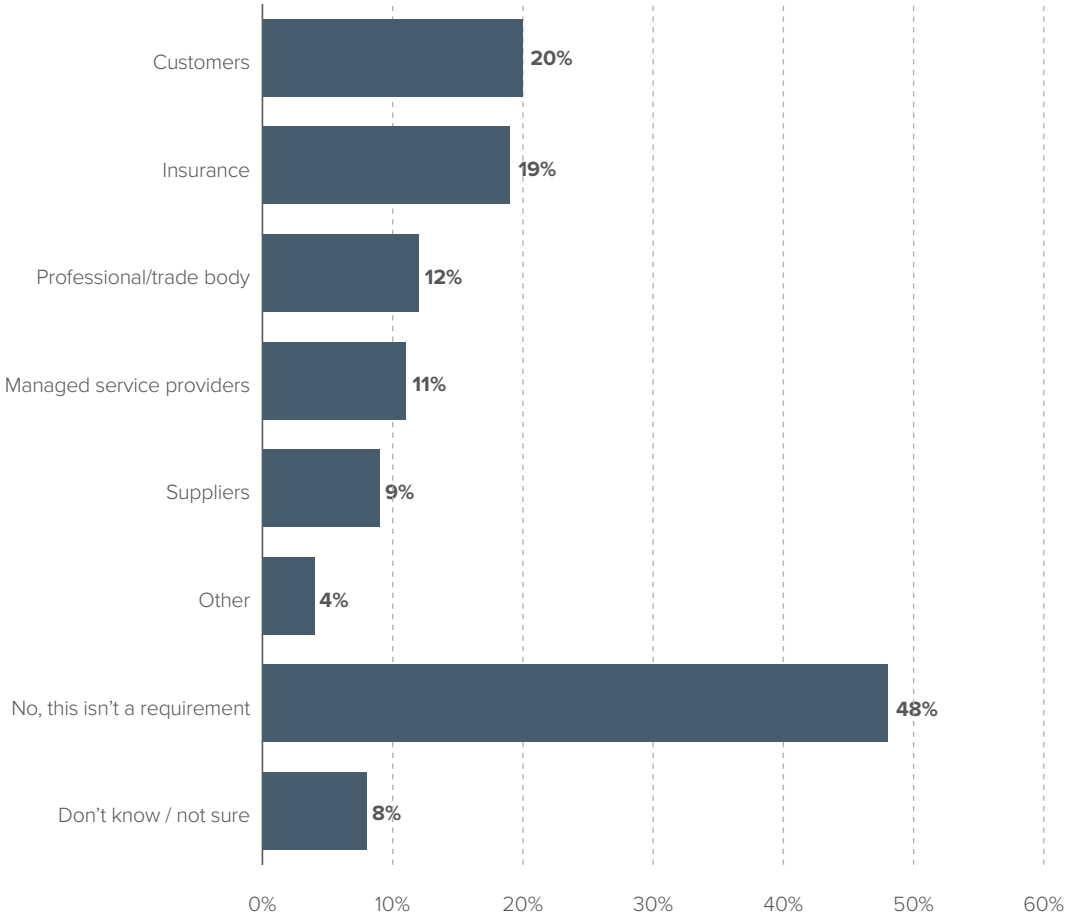
More than half (56%) of small businesses say they have invested more in cybersecurity and anti-fraud measures in the last two years. While around a third (34%) say there was no change in their level of investment and one in ten (10%) say they have not invested in any preventative measures.

It is not surprising that small businesses which have suffered from cybercrime or fraud are almost twice as likely to say they have invested more in security (66%) than those who have not (37%).

However, it is not only for businesses themselves to decide whether to invest in cybersecurity or anti-fraud measures. Requirements can also be set in the course of doing business for example by customers, or professional trade bodies. 44 per cent of small businesses say they are required to have cybersecurity or anti-fraud measures in place. Of those, a fifth (20%) say the requirement is set by their customers, 19 per cent say it is set by insurers and 12 per cent say that it is set by their professional or trade body.

Figure 14: Small businesses reporting who the requirement to have cybersecurity or anti-fraud measures is set by

Source: FSB business crime survey, 2023



Interestingly, the Government's research and analysis of the Cyber Essentials scheme published in June 2023 found the most common reason an organisation initially decides to become Cyber Essentials certified is because it is a requirement of a public sector contract (34%).[32] Previous FSB research on supply chains found that while standards can bring many benefits to businesses including consumer trust, they are often costly to implement for small businesses and complicated to comply with which can lead to a diversion of resources from running the business.[33]

Small businesses also report barriers when thinking about investment in cybersecurity or anti-fraud measures. One in five (21%) small businesses say the cost of managed service providers is too high, followed by the high cost of relevant software (19%) and not having the resources or skills to invest (15%).

"The cost of software has always been a barrier for me...so it's something I always question about whether I actually need it or not. That said, I have Malwarebytes on all my computers, which is a paid subscription and I run antivirus software."

FSB member, Lighting consultant, East Midlands

Figure 15: Small businesses views on investment in cybersecurity or anti-fraud measures
Source: FSB business crime survey, 2023

View on investment	Amount of small businesses
Cost of managed service provider is too high	21%
Cost of relevant software is too high	19%
I don't have the resources and / or skills to invest	15%
I cannot afford it due to other business costs rising	14%
I don't understand cyber security or have enough information to make a decision to invest	12%
I have never faced any issues with cybercrime and / or fraud	11%
I don't think there is a risk of cybercrime and / or fraud to my business	5%
Other	15%
Don't know / not sure	13%
None of the above / I don't think this is relevant to my business	18%

32 Department for Science, Innovation & Technology, Cyber Essential scheme process evaluation, 2023 https://www.gov.uk/government/publications/cyber-essentials-scheme-process-evaluation/cyber-essentials-scheme-process-evaluation

33 FSB report, Chain reaction: Improving the supply chain experience for small firms, 2018 https://www.fsb.org.uk/resource-report/chain-reaction-improving-the-supply-chain-experience-for-small-firms.html

Recommendations

UK Government should:

- **Establish a cross-departmental committee on tackling fraud and cybercrime.** The move online across all services including those in government means that there should be greater oversight of services particularly if they are interlinked. The cross-departmental committee would allow for more intelligence sharing across departments to better foresee any challenges for example, on coordination on any associated risks and suggestions for suitable mitigation. This could also include relevant fraud agencies and non-governmental groups.
- **Publish guidance and advice on cyber and fraud protection together with any schemes that they promote to small businesses on the use of software or other products that put them at risk of cybercrime or fraud.** Previous schemes like Help to Grow: Digital could have done more to encourage relevant cyber protection amongst businesses that used it. Any future scheme that promotes digitalisation should be supported with the appropriate cybersecurity and anti-fraud protection and advice.
- **Publish guidance for any third-party providers that provide Cyber Essentials scheme compliance to businesses to encourage them to be transparent on essential and non-essential costs in attaining the certification.** To ensure that schemes like Cyber Essentials are taken up by small businesses that need them there needs to be greater transparency over costs particularly with third party providers. Therefore, third-party providers should be clear and upfront on costs associated with different elements of certification and differentiate between the essential cost of gaining the certification and non-essential add-ons that they can provide as part of the service. Setting clearer guidelines on pricing would help to ensure that small businesses are not disadvantaged in trying to access the scheme.
- **Publish appropriate guidance and consider information campaigns aimed at small businesses to help them identify enforcement agents to ensure that they are legitimate and help to promote these through Cyber Resilience Centres.** Scams where criminals pretend to be enforcement agents have been on the rise and small businesses through fear of enforcement could be left particularly vulnerable especially if they are operating from home. Appropriate guidance and awareness campaigns could help businesses identify legitimate enforcement agents and not fall for scams.

UK Government and National Cyber Security Centre should:

- **Review the pricing of Cyber Essentials certification as well as costs associated with annual renewal in relation to the smallest businesses and explore whether lower tier pricing or a special reduced rate could be introduced.** Only 6 per cent of small businesses in our research report obtaining a recognised cyber security standard, and this is not surprising given the associated costs. Small businesses

can be disadvantaged when costs are disproportionately high, particularly in the face of other business costs rising, which can lead to them missing out on opportunities to grow and innovate. We support the latest DSIT review into Cyber Essentials and in particular the recommendation to look again at the scheme's pricing structure.

Home Office should:

- **Include the impact of fraud on small businesses in the next fraud strategy and consider a specific targeted approach with clear objectives to tackling it.** It was disappointing to see limited mention of small businesses and consideration of them as victims of fraud in the National Fraud Strategy published in 2023. Given that fraud requires a response nationally, it is imperative that the strategy is able to set the tone at the top for crimes against small businesses so that forces are aware of the impact of fraud on small businesses.
- **Make unauthorised data copying a separate offence under the Computer Misuse Act.** While unauthorised access is covered by the offence, unauthorised data copying for example, when someone copies data with the intent to sell, share or any other illegitimate use not authorised by the owner is not. Unauthorised data copying should be treated in the same way as physical theft offences, as copying of sensitive business data could lead to that data being used against the business or being sold off to competitors. Any punishments for unauthorised data copying should in line with other similar theft offences on stolen goods.

Department for Science, Innovation and Technology should:

- **Require large online services such as online platforms, social media platforms or e-mail providers to implement greater security such as multi-factor authentication to help prevent the hacking of online accounts and take action to close fake accounts on social media platforms.** Almost 1 in 10 (9%) of small businesses in our survey report having their social media account hacked, therefore platforms should have a responsibility in increasing the security of platforms as it would help prevent small businesses from being targeted. Larger companies have the capacity and capability to implement greater protection for accounts and should do so to protect their users, as this does not only impact on their profitability but also reputation. Furthermore, social media platforms should take action to rapidly close down fake accounts where there is evidence that the account has been used in attempted fraud, and resource good responsive fraud teams dedicated to a range of consumers including small businesses. Digital Markets Unit could also have a role to play in implementing this requirement on platforms designated with Strategic Market Status.

POLICING AND REPORTING CRIMES

Small businesses are an integral part of their communities. As such, small firms expect the police to be visible, provide protection, prevent crime and to prosecute criminals. All of which should be underpinned by effective Government policy.

More than two-thirds (68%) of small businesses reported the most impactful crime that they have experienced over the last two years in England and Wales to either the police, Action Fraud, the Information Commissioner's Office (ICO), their bank, or to an IT provider.

Figure 16: Reporting of most impactful crime according to type of crime
Source: FSB business crime survey, 2023

	All	Traditional	Cybercrime	Fraud
The police by phone/in-person	24%	52%	21%	24%
Single online home reporting	8%	12%	7%	8%
Action Fraud	15%	12%	16%	21%
The Information Commissioner's Office	2%	3%	2%	2%
To my bank	21%	24%	21%	34%
To the IT provider / service	19%	14%	20%	21%
Other	12%	10%	12%	12%
I did not report it	31%	18%	34%	20%

Of those that reported the most impactful crime, almost a third (31%) reported their most impactful crime to the police (either by phone, in-person or via the single online home reporting platform).

The online single home reporting hub was established in 2019, at which time FSB called for the rollout to be accelerated. Although 41 out of 43 police services nationally are committed to the platform with 34 forces fully signed up and operational already, our research shows only (8%) of small firms reported crimes via the hub in comparison to other methods of reporting such as via phone and in person reporting (24%).

Police face unfunded and unpredictable cost pressures such as cybercrime, fraud and terrorism. The under-resourcing of police forces unsurprisingly leads fraudsters to feel that they face very little risk of being caught. In addition, many victims of cybercrime and fraud feel embarrassed to report crimes, thus many cybercrimes go unreported.

It is widely understood that police need reporting data to be able to allocate resources appropriately, help to catch perpetrators and help identify organised crime groups. However, with many crimes going unreported for various reasons or being reported to others such as banks, there is a risk that the data the police currently hold is insufficient to appropriately target crime.

"We experienced courier fraud a couple of years ago. Because it was a courier we had difficulty finding actually which police force to report it to which was a nightmare. I must have spent the best part of half a day trying to report it, and to be frank, it was a complete and utter waste of time. I'd rather be part of a solution, than continue to complain about our problem, but it must completely skew statistics for police forces, because I'm sure many of the businesses are just saying actually, it's better to use my time more productively than to report stuff that I know isn't going to go anywhere."

FSB member, Governance, risk and compliance business, West Midlands

Unreported crimes

The crime survey for England and Wales is a vital source of information on the changing levels of crime and a useful monitor in the evaluation of crime reduction policies. Recorded crime data is useful in identifying emerging trends, and short-term fluctuations which can often become longer term trends especially where little action is taken to address them.

Reported crimes excluding fraud and computer misuse rose to 5.5 million offences and fraud and computer misuse crimes rose to 1.2 million offences, a rise of 15 per cent between 1 April 2022 and 31 March 2023.[34] However, unreported crimes continue to be a significant problem. Of those that had suffered any type of crime (traditional, cybercrime or fraud), around a third (32%) say they did not report it the crime. This is a significant increase on the 21 per cent who said they did not a report any type of crime in our 2019 survey.

Underreporting varies according to the crime suffered; smaller businesses that have experienced cybercrime are more likely to say they did not report the crime (34%) than those who have experienced fraud (20%) or traditional crime (18%).

Reasons for not reporting a crime vary amongst small businesses. 43 per cent of small businesses say they did not report a crime because they did not think that it was serious enough to report, and a fifth (20%) did not report it because of lack of confidence in the police or Action Fraud. Lack of confidence also differs according to crime experienced, those who have experienced traditional crime being more likely (31%) to say that they did not report a crime due to lack of confidence in the authorities than those who have experienced fraud (24%).

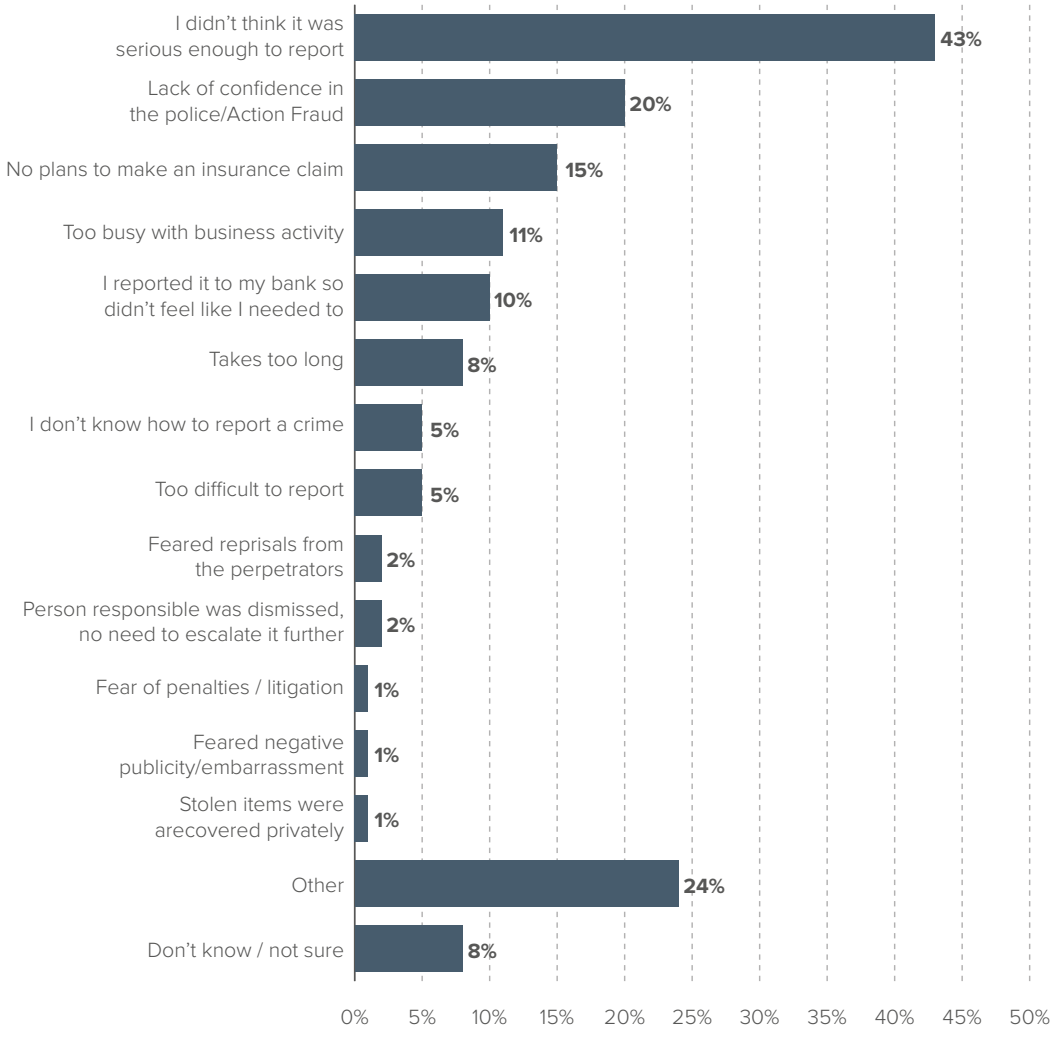
"The office has got a metal gate with a padlock on it and we've had someone attempt entry there to the point they damaged the padlock... We didn't want to report it, because the most they've done is just damage a padlock, so we just repaired the damage."

FSB member, IT management business, East Midlands

34 Home Office, Crime outcomes in England and Wales 2022 to 2023, 2023, https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2022-to-2023/crime-outcomes-in-england-and-wales-2022-to-2023

Figure 17: Reasons for small businesses not reporting crime in the last two years

Source: FSB business crime survey, 2023



Twenty-four per cent of small businesses in England and Wales stated other reasons not identified in Figure 17 for not reporting crime. These included not knowing where to report and that the crimes were originating from other countries. Some small businesses also cited concerns around lack of response and action from Action Fraud and the police.

"Our business lost money after someone gained access to one of our accounts. We reported it to Action Fraud, but they were basically useless. They did absolutely nothing. Might as well not have bothered wasting my time with it. I've never heard a word from them."

FSB member, Manufacturing business, East of England

"[Speaking in relation to bank fraud] ...I moved banks so it got sorted, but Action Fraud were totally disinterested and police totally disinterested. We have problems. We report them. But nobody actually does anything to nip it in the bud. They shrug their shoulders. They might pay some money back, but nobody in authority actually cares."

FSB member, Consultancy business, North West England

The National Fraud Strategy published in May 2023 reinforced the commitment to replace Action Fraud with a new system to help report cybercrime and fraud to the police, with a commitment from the Home Office to spend over £30 million over three years, to replace and improve the service.[35] The strategy highlights that the new service will make it much easier to report crime online, access advice, and track progress of reports, as well as commits to the launch in a year's time in 2024. It will also include an upgraded call centre that will reduce waiting times.

While it is positive to see steps taken to make it easier to report and track crimes, some small business owners expressed concerns around the new plans, with some stating the lack of information given (a crime number but no further updates) which then leads to a lack of confidence in reporting a crime. Additionally, small businesses have concerns whether these plans can be resourced properly, especially in tackling fraud and cybercrime.

A fifth of small businesses say that they did not report a crime to either police or Action Fraud because of lack of confidence. YouGov's police confidence tracker shows the proportion of people who have a fair amount of confidence in the police to deal with crime, as of September 2023, this figure stood at 38 per cent.[36]

Our research shows of the smaller businesses in England and Wales that reported a crime, 59 per cent say the police did not attend the scene, increasing to 61 per cent of who reported their most impactful traditional crime. This is a significant increase on 2019, in which 48 per cent stated the police did not attend the scene.

35 Home Office, Fraud strategy: Stopping scams and protecting the public, 2023 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154660/Fraud_Strategy_2023.pdf

36 YouGov, How much confidence Brits have in police to deal with crime, 2023 https://yougov.co.uk/topics/politics/trackers/how-much-confidence-brits-have-in-police-to-deal-with-crime

Figure 18: Initial response to a police report

Source: FSB business crime survey, 2023

Initial response to a police report	Percentage of small businesses reporting
Did not provide a crime number and did not attend	22%
Crime number provided but did not attend	39%
Discussed it over the phone but no crime number was given	12%
Discussed it over the phone and crime number was given	11%
Sent an officer within an hour	5%
Sent an officer within 3 hours	5%
Sent an officer within 24 hours	4%
Sent an officer within a week	5%
Sent an officer after 7 days	3%
None of the above	12%

"Any crime, no matter how small, we report to the police, but we don't expect any action from the police. In the past, we've had the break in to the premises where there's been clear footprints, fingerprints and all sorts. The police wouldn't even go and look at them which doesn't instil confidence in one. There was no result from that either, just that was about £20,000 worth of stuff taken and damage to the premises from breaking in."

FSB member, Manufacturing and construction company, North West England

Close to half (48%) of small businesses report that the police did not investigate the crime reported; this figure increases to 53 per cent for small firms based in urban areas in England and Wales. Only in 3 per cent of cases the police investigated, identified and arrested the perpetrators.

Figure 19: Outcome following the initial police response

Source: FSB business crime survey, 2023

Outcome following the initial police response	Percentage of small businesses reporting
The police did not investigate	48%
The police investigated, but could not identify the perpetrators	18%
The police investigated and identified the perpetrators, but could not / did not arrest them	10%
The police investigated, identified and arrested the perpetrators	3%
Don't know / not sure	7%

Small firms are integral to their local communities as such their views on local policing are invaluable. Our research suggests the police are under-resourced to deal with cases of small business crime.

Policing resources

Previous FSB research highlighted gaps in police funding and the continued decrease in the number of police officers that are available to deal with crime. With that said, since the government's commitment to employ 20,000 more officers in 2019, the number of police officers has increased with the number of full-time equivalent (FTE) officers across the 43 forces standing at 149,566 as of March 2023, meaning that that there are only 251 police offers per 100,000 in England and Wales. This is still significantly below the European average of 335 police officers per 100,000.[37]

This not only makes it more difficult to tackle traditional crime but complex and evolving crimes such as fraud which the police have less experience in tackling. Increasing the number of police would help to act on their commitments on hot spot policing delivering the anti-social behaviour strategy as well as ensure that there are enough resources to focus on business crime.

"If you're victim of a crime and you report it, what are you going to get? Most probably a crime number, and that's it. There is a big education [piece] that has got to be done, and it will mean involving the police...the police are really under resourced."

FSB member, Management consultancy, East Midlands

37 Eurostat, Police, court and prison personnel statistics, 2023 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Police,_court_and_prison_personnel_statistics

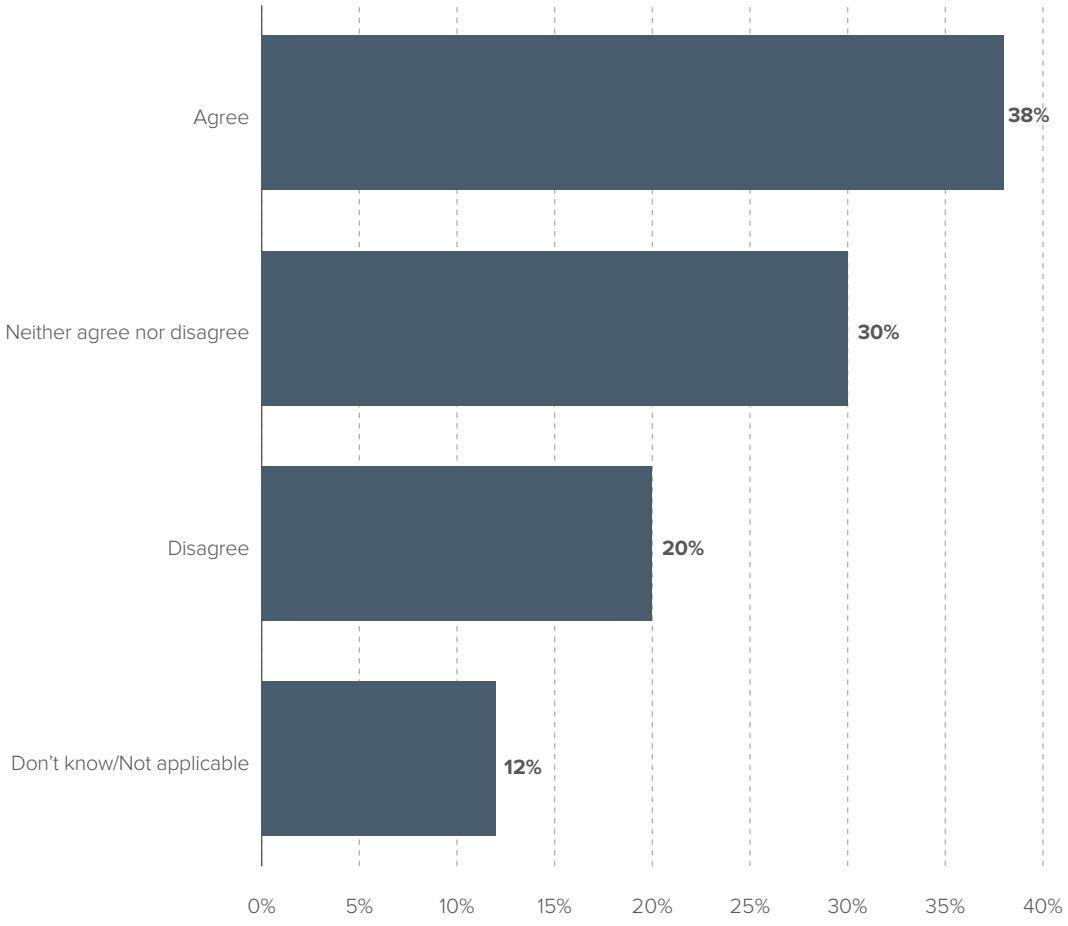
Community policing

Small businesses are also supportive of introducing more Police Community Support Officers (PCSOs) as a way of encouraging greater police presence. PCSOs were introduced in 2002, to provide support to police officers and play a vital role in understanding the challenges of communities in relation to crime.

Small businesses want to see consistent and proactive neighbourhood policing. More than a third (38%) of small businesses agree that increasing the number of PCSOs would help to tackle business crime. A fifth (20%) disagree.

Figure 20: Extent to which small businesses agree or disagree that increasing the number PCSOs will help tackle business crime in their local area

Source: FSB business crime survey, 2023



At present only around one per cent of police personnel are dedicated to fraud, and of government's promised 20,000 new police officers, only 380 will specialise in fraud.[38] Law enforcement will never be able to effectively deal with fraud without increasing the police capacity and capability, including greater collaboration locally and internationally. However, forces have also reported difficulties in recruiting and retaining individuals with specialist skills due to their desirability in the private sector.[39]

Tackling fraud and online crime requires capabilities, coordination and oversight on a national basis. There have been steps taken to ensure that this happens for example, through City of London Police being the lead force on fraud response and the National Economic Crime Centre (NECC) to help tackle serious and organised crime. However, given that investigations are often conducted locally but the responsibility for overall approach to fraud is central, there have been calls to better define and outline the responsibilities of local forces and the support available to local forces from centralised bodies.[40] The National Fraud Strategy also announced the launch of a National Fraud Squad (NFS) with a focus on high-end fraud and organised crime.

Since the Police Scotland merger in 2013, there have been calls to consider police force mergers in Wales, as well as in England. The benefits cited in access to data and systems to ensure better policing, as well as help to ensure that there would be greater access to senior talent. However, given the size of the police force in Scotland being around a half of that only of Metropolitan Police, it could be that any merger in England could potentially lead to greater disruption. Careful thought would need to be given to any forces that may benefit from merger, as it is clear that a single unified approach across England and Wales may not be successful.

It is important to ensure that police resources are deployed correctly and underpinned by clear and targeted strategies which adequately address the needs of small business crime – at the heart this needs to be underpinned by an effective police recruitment and retention plan.

There are also other ways to free up police resources. For example, the announcement to free up more police resources through cutting unnecessary red tape in crime recording processes is welcome.[41] Further reductions in bureaucracy would also help police to effectively tackle crime. This could include the introduction of new technology to speed up administrative work, or a collaborative approach with existing data and systems could enable the police to better classify data. For example, if a crime is classified as a business crime, then the company and the director including their contact details could be populated from Companies House data. A clearer classification of data could lead to greater efficiencies when allocating resources, particularly in relation to business crime.

38 Committee of Public Accounts, Progress combatting fraud, 2023 https://publications.parliament.uk/pa/cm5803/cmselect/cmpubacc/40/report.html

39 *Ibid.*

40 Justice Committee, Fraud and the Justice System inquiry, 2022 https://committees.parliament.uk/work/1690/fraud-and-the-justice-system/publications/

41 Home Office, Police given more time to focus on solving crimes and protecting public, 2023 https://www.gov.uk/government/news/police-given-more-time-to-focus-on-solving-crimes-and-protecting-public

There is currently no mandatory recording process for business crime,[42] and although some forces do apply a business flag to their recorded crime voluntarily,[43] this leads to a fragmented approach across forces and the true extent of crime against businesses remains hidden. No accurate recording means that business crime continues to be treated as invisible crime with losses associated with just expected to be absorbed. Lack of accurate data and the true extent of business crime, not only leads to difficulties around being able to identify perpetrators or organised crime gangs particularly those that only target businesses for example through specifically targeting industrial estates, farm equipment or running shop theft gangs, but also to a lack of accountability against progress on business crime forces. The gap in statistical data also means that business crime is also noticeably absent from the Crime Outcomes for England and Wales statistics.[44]

42 Home Office, Home Office Crime Recording Rules for frontline officers & staff, 2023 https://www.gov.uk/government/publications/counting-rules-for-recorded-crime

43 College of Policing, Policing business crime, 2015 https://www.college.police.uk/app/investigation/policing-business-crime

44 Home Office, Crime outcomes in England and Wales 2022 to 2023, 2023, https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2022-to-2023/crime-outcomes-in-england-and-wales-2022-to-2023

Recommendations

Home Office should:

- **Introduce a mandatory recording process for business crime and add a 'business crime' section to the crime outcomes in England and Wales statistics so progress can be tracked, and targets set.** This could be done initially by adding a business crime option to Action Fraud reporting system or the single online home reporting system while the in-person/by-phone options are rolled out. Ensuring that business crime is recorded appropriately will help to demonstrate the crime outcomes but also compare these to outcomes of other crimes, including in tackling better outcomes for businesses and shifting perceptions of the impact of business crime.
- **Aim to increase the average number of police officers in England and Wales up to 335 per 100,000 population to help dedicate appropriate resources for crime against businesses including cybercrime and fraud.** As of March 2023, there were 149,566 full-time equivalent (FTE) police officers, which is equivalent to 251 police officers per 100,000 population in England and Wales. The 20,000 increase in the number of police officers has been welcome as part of Government's commitment of police uplift. However, this is still very short of the average level across Europe. This is particularly important given the previous Home Secretary's encouragement for police to follow up on all reasonable lines of enquiry and for no crime to be ruled out as minor including ASB and theft.
- **Use the data collected by new Action Fraud reporting system, which is due to be launched in 2024, when allocating resources nationally between forces and encourage the same within police forces.** Aside from the transparency introduced into the new system which will show progress of fraud reports to foster greater trust of public and businesses, ensuring that the system is able to directly feed into resources nationally and locally could help to ensure greater accountability.

National Police Chiefs' Council should:

- **Cut red tape for police forces, to allow them to focus on solving crime.** The National Police Chiefs' Council found that 443,000 officer hours are spent filling in unnecessary forms and burdensome administrative tasks.[45] Further efficiencies could be made particularly in light of the Companies House reforms that will include ID verification and accurate information on businesses, which could be used to save time on making reports. More extensive use of other government-controlled datasets or collaboration with or references by (for instance) banks to detect early stages of criminal activity and identify suspects should also be considered.
- **Commit to attending the scene of incidents of traditional business crime where there has been an aggravating factor such as violence or damage to premises, and progress should be tracked and reported for accountability.** In 2022, NPCC committed to attending all home burglaries which has been achieved a year later.[46] [47] Our research shows that in 59 per cent of cases police did not attend the scene, increasing to 61 per cent for those that reported traditional crime. While we recognise that it may not be possible to attend in all circumstances, a commitment should be made to attend as swiftly as possible where violent behaviour has been reported or damage done to property.

45 Home Office, Police given more time to focus on solving crimes and protecting public, 2023 https://www.gov.uk/government/news/police-given-more-time-to-focus-on-solving-crimes-and-protecting-public

46 National Police Chiefs' Council, All home burglaries will be attended by the police, 2022 https://news.npcc.police.uk/releases/all-home-burglaries-in-england-and-wales-will-be-attended-by-the-police

47 National Police Chiefs' Council, Police now attending scene of every home burglary, 2023 https://news.npcc.police.uk/releases/police-now-attending-scene-of-every-home-burglary

METHODOLOGY

The research that this report is based on was two-fold. It consisted of a survey of small businesses, along with sector-specific focus groups and one-to-one interviews to better understand the experiences of FSB members in England and Wales in relation to business crime. Members were asked to participate in the research through email invitations.

The survey was administered by the research agency Verve and was in the field from 2nd March – 20th March 2023. The survey received 560 responses and the findings were weighted to make them representative for FSB membership. All percentages have been rounded up to the nearest percentage point, which is why may some of them may not add up to 100 per cent.

The focus groups took place via Zoom, and the majority of participants were sourced through recontact data from the survey, while others were from appeals for participants within the FSB membership via email. The participants were purposefully drawn from a number of regions.

fsb.org.uk

FSB Westminster

@fsb_policy

@fsb_uk

If you require this document in an alternative format please email: accessibility@fsb.org.uk

This report can be downloaded from FSB's website at www.fsb.org.uk