DELIVERING GROWTH

INVESTMENT

CRIME AGAINST BUSINESS:

The Hidden Threat to UK Growth

British Chambers of Commerce

WHERE BUSINESS BELONGS

CONTENTS

1. Key Recommendations 04
2. Executive Summary 05
3. The Extent of Business Crime in England and Wales 06
4. Sectoral Analysis: Differential Impact 08
5. The Impact on Growth and Operations 10
6. Current Challenges in Tackling Business Crime 11
7. The Scale, Impact and Cost of Serious Organised Crime on UK Businesses and Growth 13
8. Policy Recommendations 14
9. Conclusion 16

1. KEY RECOMMENDATIONS

The Department for Science, Innovation and Technology

To reduce the reporting burden on businesses during cyber incidents:

Implement a "Report Once, Protect Many" Cyber Intelligence Policy. Enhance, where possible, information sharing between the Information Commissioner's Office (ICO) and the National Cyber Security Centre (NCSC), to ensure that any cyber breach reported is triaged to the NCSC for threat disruption. This would give businesses a single reporting gateway during a crisis while enabling intelligence-led protection.

The Home Office

To end chronic under-reporting and make data work for businesses:

Establish an intelligent, tiered reporting ecosystem. This system should firstly accredit third-party reporting hubs for non-emergency incidents. Secondly it should create automated reference-only routes for insurance-related reports. Thirdly it should provide businesses with feedback showing how their reporting data has informed local enforcement activity and hotspot mapping.

To shift forces toward community-focused issues and reduce policing costs:

Create Regional Business Crime Hubs, co-funded by police forces and Business Crime Reduction Partnerships (BCRPs), with a clear division of labour. BCRPs lead on engagement, prevention and victim support. Police forces should focus strictly on high-harm offenders and organised theft rings, reducing cost while leveraging private sector expertise.

To build the evidence base for stronger national action on business crime:

Commission a National Business Crime Strategic Assessment aligned with National Crime Agency (NCA) analytical standards. The project should evaluate the total economic harm and links to serious organised crime, forecast emerging threats, such as commercial fraud and supply chain disruption, and identify capability gaps to justify resource reallocation.

To improve business resilience against cyber crime and fraud:

Scale the existing regional Cyber Resilience Centre network by funding its expansion into Business Resilience Hubs. The hubs should provide integrated cyber and fraud support, alongside subsidised micro-business training based on Cyber Essentials, plus an additional fraud prevention component.

2. EXECUTIVE SUMMARY

Business crime represents a significant measurable constraint on UK economic growth, yet it remains chronically under-prioritised in both policy-making and resourcing.

This report focuses on England and Wales due to data availability and the policy levers held at Westminster. However, the findings are indicative of a wider UK challenge, given the integrated nature of business activity, supply chains and investment across the economy.

BCC data from October 2025 shows 42% of UK businesses experienced crime in the past year, encompassing theft and burglary, cyber-attacks, and fraud and scams. Victimisation scales sharply with firm size:

- Micro-businesses (under 10 staff) experience crime at a rate of 32%.
- Among large firms, of 250 or more employees, this rises to 58%.

Despite this scale, only 55%-58% of victimised businesses report incidents to police, meaning official statistics capture less than half of actual offences. Serious organised crime compounds the picture, costing the UK economy at least £47bn annually.

The economic consequences extend beyond direct losses. Retailers alone invested a record £1.8bn in crime prevention 2023/24, a 50% year-on-year increase, diverting capital from productive investment. Fraud, cyber-attacks and operational disruption collectively erode productivity, suppress business confidence and deter both domestic expansion and inward investment.

To mitigate this escalating threat and safeguard economic stability, government must adopt a strategic, whole-system approach:

- **Streamline Cyber Reporting**
  Implement a "Report Once, Protect Many" cyber intelligence policy, establishing automatic data sharing between the Information Commissioner's Office (ICO) and National Cyber Security Centre (NCSC) to ease the regulatory burden during crises.
- **Combat Under-Reporting**
  Establish an intelligent reporting ecosystem that utilises accredited third-party hubs and automated routes to capture vital hotspot data.
- **Transition Policing Models**
  Create Regional Business Crime Hubs, co-funded by policing and Business Crime Reduction Partnerships (BCRPs), allowing police to focus on high-harm offenders.
- **Build the Evidence Base**
  Commission a National Business Crime Strategic Assessment aligned with National Crime Agency (NCA) standards to accurately evaluate economic harm and guide resource reallocation.
- **Enhance Local Defence**
  Scale the existing regional Cyber Resilience Centres into integrated Business Resilience Hubs to provide micro-businesses with subsidised cyber and fraud training.

Without decisive intervention, business crime will continue to function as an unacknowledged brake on UK growth.

3. THE EXTENT OF BUSINESS CRIME IN ENGLAND & WALES

Overall Prevalence

Business crime has become commonplace.

BCC survey data from 2025 shows 42% of UK firms experienced some form of crime in the past year; however, even these figures undercount the problem.

Only 55-58% of victimised businesses report incidents to police[i], meaning official statistics capture barely half of actual offences. This reporting gap, the 'dark figure' of crime, confirms business crime's status as a hidden economic threat, one whose true scale and cost remain systematically under-measured.

Under-reporting concentrates among smaller firms, high-street retailers and businesses facing high-volume, low-value offences. For many, repeated theft, vandalism or online fraud has become background noise, not worth the administrative burden of reporting. Others doubt that reporting achieves anything. The feedback loop is self-reinforcing: low reporting produces low prioritisation, which validates business cynicism, which suppresses reporting further.

Physical Crime: The Persistent Threat

Physical crime remains persistent and rising. BCC research from last year shows 15% of businesses experienced theft, burglary or vandalism in the past year, but this average conceals sectoral variation, with consumer-facing businesses hit at 22%, highlighted in the same data set.

Police data confirms the recent trend that shoplifting and robbery against businesses have surpassed pre-pandemic levels. The 2023 Crime Victimisation Survey (CVS) similarly identifies theft as the most common offence, affecting 14% of premises[ii]. Despite advances in security technology, physical assets remain highly vulnerable and the threat is intensifying rather than receding.

Retail and hospitality face the sharpest increases. Police-recorded shoplifting reached 516,971 offences in the year to December 2024, a 20% year-on-year rise and the highest figure since current recording began[iii]. By March 2025, the total exceeded 530,000.

These headline numbers hide the fact that certain premises, like supermarkets and convenience stores, face several incidents each day rather than just once a year.

Cyber Crime: The Digital Front

As business operations digitise, so does the threat. BCC research from 2025 shows 21% of firms experienced cyber-attacks (hacking, phishing, ransomware) in the past year, with near-uniform distribution across sectors (20-23%). No sector is immune from attacks. The 2025 Cyber Security Breaches Survey, which reflects a broader definition that captures any attempted breach, including those blocked by routine defences, confirmed 43% of businesses reported having any kind of cyber security breach or attack in the last 12 months[iv].

The economics differ fundamentally from physical crime. A single ransomware attack can paralyse operations entirely, creating losses that dwarf typical theft. Sophistication is rising, with smaller firms increasingly exploited as supply chain entry points to larger targets.

Government survey data shows that while overall cyber-crime prevalence has remained relatively stable, ransomware incidents have doubled in a year, from under 0.5% of all businesses in 2024 to around 1% in 2025, equivalent to an estimated 19,000 firms[v].

Fraud and Scams

Fraud operates invisibly. BCC data from last year shows 20% of businesses experienced fraud or scams in the past year, but unlike physical crime's immediate visibility (broken windows, missing inventory), fraud often goes undetected until long after losses occur.

The distribution reveals sophistication. Within the BCC's survey manufacturing and consumer-facing services report rates of 24-25%, reflecting industrialised schemes such as invoice fraud, CEO impersonation and procurement scams. These aren't opportunistic crimes; they're systematic revenue streams for organised criminal operations.

Organisation Size Matters

BCC research from 2025 reveals that micro-firms (under 10 staff) face the lowest crime rates, with 32% experiencing some form of crime, while large firms (250+ staff) face the highest rates at 58%. This pattern aligns with CVS findings that larger premises experience a higher victimisation rate and reinforces a simple truth. As organisations grow, their risk surface and the opportunity for offenders expand.

4. SECTORAL ANALYSIS: DIFFERENTIAL IMPACT

Business crime concentrates unevenly across sectors, creating distinct risk profiles that demand targeted policy responses.

Manufacturing

Manufacturing contributes disproportionately to UK productivity and exports while enduring disproportionate criminal targeting.

Prevalence

BCC data shows that 50% of manufacturing firms experienced some form of crime in the last year. Among the four sectors surveyed – manufacturing, B2B, B2C and public, third, health and education – manufacturing was the hardest hit.

Risk Profile

Manufacturers face convergent threats across three dimensions. Valuable physical assets, raw materials, machinery, inventory, produce an 18% physical crime rate. Multi-tier supply chains create fraud opportunities, affecting 25% through invoice manipulation. Meanwhile, operational technology digitisation exposes 23% to cyber-attacks targeting production systems.

Impact

Physical and digital crime create distinct damage patterns. Theft of copper, machinery and materials increases production costs. Cyber-attacks on operational technology systems halt production, propagating delays through supply chains.

B2C Services (Retail, Hospitality, Leisure)

B2C services face the highest crime exposure on the high-street, with retail and hospitality particularly vulnerable.

Prevalence

46% of B2C firms encountered crime, with the highest physical crime rate of any sector at 22%, as highlighted in the BCC's 2025 survey.

Risk Profile

Government data shows wholesale/retail premises suffer crime at 41-42%, nearly double the cross-sector average[vi].

Impact

Shoplifting has reached epidemic levels, affecting 26% of retail premises[vii]. The problem extends beyond inventory loss. Rising violence against staff deters town-centre investment and worsens the sector's labour crisis.

B2B Services (Professional Services, Finance, Tech)

Office-based and remote operations might seem insulated from crime, but B2B firms face substantial exposure.

Prevalence

As documented in the BCC's 2025 research, physical crime is rare for B2B firms (11%), but overall victimisation hits 39%. The gap reveals where the threat actually concentrates, fraud and cyber-attacks, rather than theft.

Risk Profile

Digital and financial threats dominate. 19% experienced fraud, 22% cyber-attacks.

Impact

B2B firms face a different threat calculus. A 'break-in' means stolen credentials, not broken locks. Lost client data or intellectual property triggers reputational damage and regulatory fines severe enough to end businesses, particularly SMEs operating on thin margins of trust.

Public and Third Sector (Health, Education, Charities)

Crime against public sector and charitable organisations diverts taxpayer funding and donations away from essential services and social good.

Prevalence

Shown in BCC's Survey Data crime affects 42% of these organisations, nearly matching retail despite fundamentally different exposure patterns.

Risk Profile

Physical incidents (20%) often involve vandalism of schools or theft of medical equipment. Cyber threats are escalating, evidenced by high-profile ransomware attacks on the NHS.

Impact

These crimes produce social casualties, not just financial losses. Hospital cyber-attacks mean postponed surgeries and compromised patient care. Charity fraud converts donations into criminal proceeds.

5. THE IMPACT ON GROWTH AND OPERATIONS

Business crime functions as a macroeconomic drag, not merely a policing problem. The cumulative effect slows UK growth across multiple channels.

Direct Financial Losses

Business theft operates as a pure economic transfer from legitimate commerce to criminal actors. The Home Office estimated crime against businesses in England and Wales cost firms £9bn a year a decade ago[viii], a figure that has almost certainly risen substantially, given today's escalating retail losses and cyber-fraud.

Annual fraud losses alone reach billions, compounded by hundreds of thousands of theft incidents. For small businesses, the impact isn't statistical; it's existential. One £10,000 fraud can exhaust working capital, trigger debt default and force closure.

The Opportunity Cost of Security

Faced with rising levels of crime, businesses divert investment from productive to protective uses.

Retailers invested a record £1.8bn in crime prevention during 2023/24, a 50% increase from £1.2bn, diverting resources from expansion and productivity gains[ix]. The convenience sector alone spent £339m on prevention measures in the past year. The cumulative burden of this retail crime effectively adds approximately 10p to every transaction: a tangible, economy-wide tax on growth that consumers ultimately bear[x].

Money that could fund innovation, skills development or expansion instead pays for cameras, guards and cyber defences. This defensive spending maintains the status quo while competitors in lower-crime environments invest in growth.

Operational Disruption and Productivity

While direct financial losses are quantifiable and visible, the indirect costs of business crime often inflict deeper, longer-lasting damage. These operational disruptions act as a hidden drag on efficiency, consuming resources that cannot be easily replaced.

Recent government survey data revealed that 43% of UK businesses suffered a cyber breach or attack in the last 12 months[xi]. For incidents that resulted in financial losses, businesses faced an average cost of approximately £3,550, a figure that encompasses downtime, recovery efforts and incident response[xii].

Expanding beyond the balance sheet, these disruptions ripple through customer relationships, workforce morale and strategic decision-making. Time spent on incident response, securing premises, rebuilding systems, dealing with insurers and communicating with stakeholders is time not spent serving customers or innovating. The cumulative effect is slower productivity and a persistent drag on competitiveness.

Erosion of Confidence

Crime against individuals and households has generally declined over the past decade, with fraud emerging as a significant exception. Fraud now represents a substantial proportion of all crime against individuals. 4.2 million incidents were estimated in the year ending September 2025[xiii], with bank and credit account fraud increasing by 19% to 2.6 million incidents. This surge in fraud helps explain why both consumers and businesses have adopted more cautious online behaviours, including slower transaction processing and stricter authentication measures.

Growth requires confidence in transactional security. Crime undermines this foundation through visible disorder (shoplifting deterring high-street visits) and invisible risk (fraud suppressing online commerce). The combined effect slows spending velocity, discourages business formation and redirects investment capital toward less risky markets.

6. CURRENT CHALLENGES IN TACKLING BUSINESS CRIME

The disconnect between crime's economic impact and policy response reflects structural barriers that have prevented effective intervention.

Under-Reporting and Data Gaps

Business crime's invisibility is self-reinforcing. With 42-45% of victimised businesses not reporting to police, data-driven resource allocation models systematically under-count the problem, producing inadequate enforcement response[xiv]. This validates business cynicism about police effectiveness, which suppresses reporting further.

Businesses don't report for two reasons. Incidents seem too minor to warrant police time, or past experience suggests reporting achieves nothing. Both perceptions, whether accurate or not, ensure the cycle continues.

Limited Police Resources and Prioritisation

Enforcement priorities reflect resource constraints and public expectations. Crimes against individuals, especially violent offences, command attention and resources. Business crimes, particularly fraud and cyber-attacks, fall lower in the hierarchy regardless of overall economic harm.

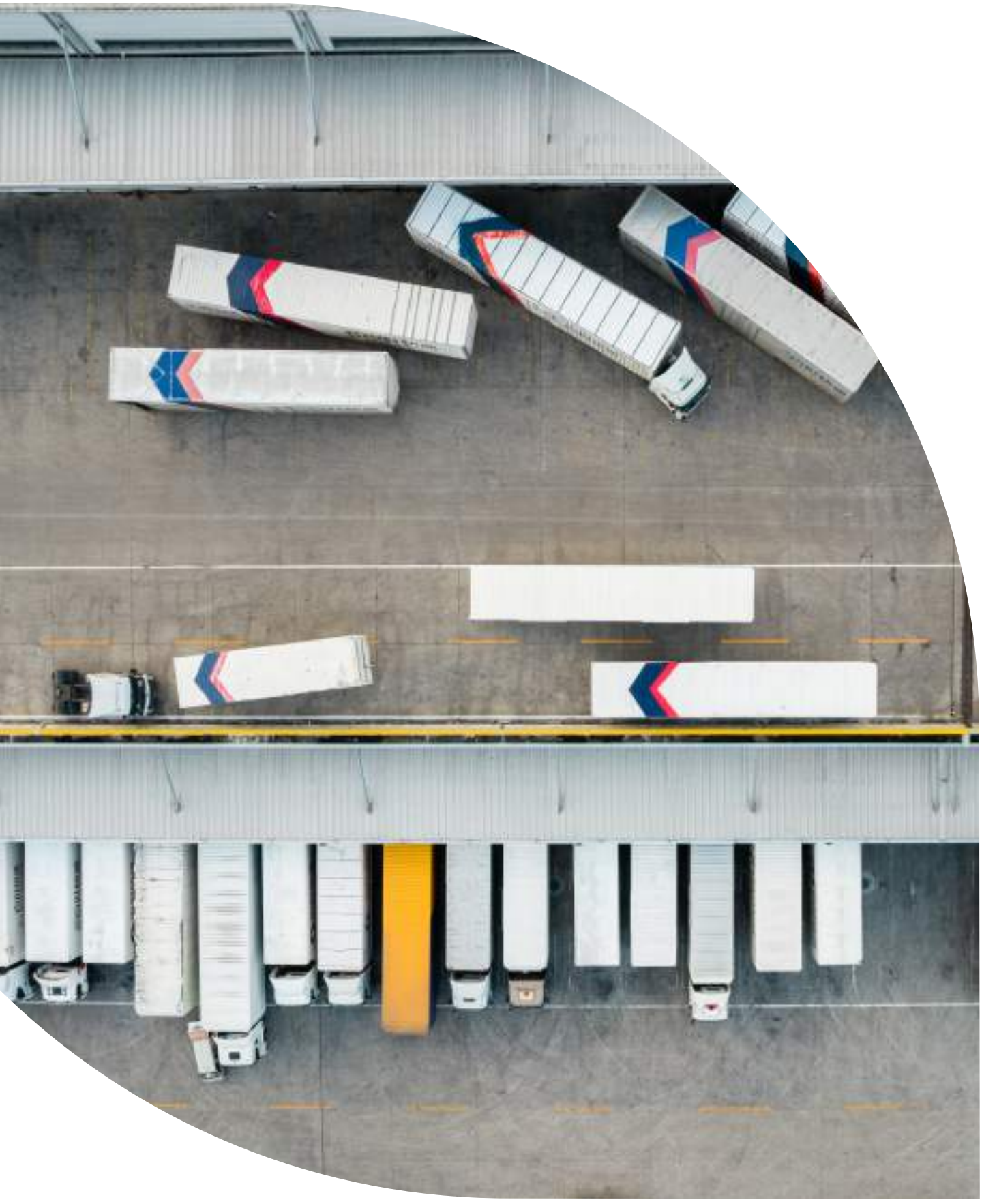
- Government data from 2023 shows only 35% of businesses were satisfied with the police response when they did report crimes[xv].
- 63% of dissatisfied businesses cited that 'police never showed up' or 'did nothing'[xvi]. This breach of the social contract between the state and enterprise discourages future reporting.

Sophistication and Volume

The nature of crime has evolved faster than the response, with fraud now the dominant crime type by volume. The Office for National Statistics (ONS) reports a 22% rise in fraud[xvii]. Within the same time frame, consumer and retail fraud has risen 49%.

Automated cyber-attacks and international fraud rings operate at a volume that overwhelms traditional constabulary policing.

The UK is attempting to fight 21st-century digital industrialised crime with inefficiently resourced local policing structures.



7. THE SCALE, IMPACT AND COST OF SERIOUS ORGANISED CRIME ON UK BUSINESSES AND GROWTH

Serious organised crime (SOC) constitutes one of the most substantial threats to national security and economic stability facing the UK.

The National Crime Agency (NCA) estimates SOC costs the UK economy at least £47bn annually[xviii], compromising productivity, competitiveness and business confidence.

This is compounded by the UK's role as a financial and logistical hub for criminal networks. Over £100bn is laundered through UK corporate structures, and a further £12bn in illicit proceeds is generated domestically each year[xix].

This exposes legitimate enterprises to infiltration, fraud and reputational damage.

The NCA confirms SOC continues to escalate in scale, sophistication and technological capability, representing a persistent threat to UK economic resilience.

Scale and Nature of Threat

SOC affecting UK businesses is characterised by:

- Escalating financial crime, with criminals exploiting professional services, crypto assets and complex corporate structures to conceal illicit funds.
- Fraud, the most frequently reported offence in the UK, generating losses of billions annually through push payment fraud, investment schemes, phishing and AI-enabled social engineering.
- Increasing exploitation of UK businesses, either knowingly or unknowingly, as conduits for illicit finance, sanctions evasion and the obfuscation of beneficial ownership.

Impact of SOC on UK businesses:

- Financial losses from fraud, cyber-enabled crime and infiltration of financial systems by organised criminal networks.
- Operational disruption through AI-driven phishing and sophisticated financial crime targeting supply chains and digital infrastructure.
- Regulatory and compliance pressure on firms in legal, accounting, financial services and company formation sectors, facing exploitation risk as professional enablers, with intensified scrutiny and potential liability.

The SOC threat is rapidly expanding, driven by technological innovation, exploitation of financial systems and reliance on professional enablers. Criminal networks are leveraging crypto assets, corporate structures and AI-enabled techniques to target UK businesses on an unprecedented scale.

8. POLICY RECOMMENDATIONS

To move business crime from a "hidden threat" to a prioritised economic security issue, responsibilities must be divided across the system.

1. RECOMMENDATIONS FOR GOVERNMENT

Primary Stakeholders: Home Office, DBT, DSIT and HM Treasury.

Establish the National Evidence Base

The Home Office should commission a National Business Crime Strategic Assessment to calculate total economic harm and identify capability gaps.

Expand Policy Scope

The Home Office and Department for Business and Trade (DBT) must mandate that the National Business Crime Strategy evolve beyond retail to include commercial fraud and industrial burglary.

Implement "Report Once, Protect Many" Cyber Policy

The Department for Science, Innovation and Technology (DSIT) should establish a mandatory data-sharing agreement between the Information Commissioner's Office (ICO) and the National Cyber Security Centre (NCSC) to streamline reporting during cyber incidents.

Incentivise Resilience via Tax Credits

The government should introduce a "Business Security Tax Credit" linked to accredited risk assessments to help SMEs fund physical and digital defences.

Reform Sentencing Guidelines

Encourage the Sentencing Council to consider updating its framework to account for the "multiplier effect" of business crime, such as supply chain disruption and loss of local employment.

2. RECOMMENDATIONS FOR LAW ENFORCEMENT AND REGIONAL PARTNERS

Primary Stakeholders: Police Forces, BCRPs and the NBCC.

Transition to Blended Hubs

Police forces should co-fund Regional Business Crime Hubs with Business Crime Reduction Partnerships (BCRPs), where police focus on high-harm offenders while BCRPs lead on engagement.

Modernise the Reporting Ecosystem

Law enforcement should adopt a tiered system that utilises accredited third-party hubs for non-emergencies and automated "reference-only" routes for insurance reports.

Operationalise Intelligence

The National Business Crime Centre (NBCC) must be upgraded to disseminate NCA-level intelligence on organised fraud rings directly to local units.

Deploy Data-Driven Resources

Use the reporting ecosystem to trigger joint patrols between police and Business Improvement District (BID) wardens in identified high-risk "hotspots".

3. RECOMMENDATIONS FOR THE PRIVATE SECTOR (BUSINESSES AND INDUSTRY)

Primary Stakeholders: Firms, Professional Services and Trade Bodies.

Harden Financial and Digital Defences

Businesses must implement multi-factor authentication, advanced email filtering, and more rigorous KYC (Know Your Customer) checks to defend against AI-enabled fraud.

Commit to Intelligence Sharing

Firms should participate in sector-specific forums and promptly report suspicious activity to law enforcement to improve national situational awareness.

Prioritise Material Compliance

Large firms must move beyond "tick-box" exercises to substantive supply chain security, ensuring the burden of protection is not simply passed down to smaller partners.

Invest in Staff Training

Businesses should provide mandatory fraud-awareness and cyber-hygiene training, specifically focusing on AI-generated phishing and impersonation attacks.

4. CROSS-SECTOR COLLABORATION: BUSINESS RECOVERY

Success should be measured by the "survival rate" of small firms following a major criminal incident. To achieve this, Regional Hubs must integrate specialist recovery support that helps owners navigate commercial recovery, insurance, and insolvency prevention in the aftermath of a crime.

9. CONCLUSION

Business crime is not an operational nuisance but a structural constraint, a measurable brake on UK economic performance.

The BCC's most recent survey data evidence is unambiguous: 50% of manufacturers face theft and fraud, 46% of retail businesses are hit, 42% of public and charitable organisations experience victimisation, whilst 42% of all businesses surveyed by the BCC were crime victims in the past year. The 'hidden threat' extracts tangible costs in lost productivity, diverted investment and eroded confidence.

The trajectory points toward escalation. Criminal capabilities advance alongside technology, more sophisticated cyber-attacks, more organised fraud networks and more coordinated supply chain targeting. Without policy response, the UK's business environment will deteriorate relative to competitors, making British commerce progressively less viable.

This outcome is preventable. The recommendations in this paper, strengthened enforcement, security investment incentives, unified national strategy, offer a credible intervention path. Implementation requires coordination across government, law enforcement and business, but the alternative is managed decline.

The British Chambers of Commerce and the business community are prepared to partner in this effort. Reducing business crime isn't about protecting balance sheets alone; it's about removing structural impediments to UK growth. The question is whether policy will match the urgency the data demands.

10. APPENDIX

i. Home Office – Crime against Businesses: findings from the 2023 Commercial Victimisation Survey

ii. Home Office – Crime against Businesses: findings from the 2023 Commercial Victimisation Survey

iii. Office for National Statistics – Crime in England and Wales: year ending December 2024

iv. Home Office – Cyber security breaches survey 2025

v. Home Office – Cyber security breaches survey 2025

vi. Home Office – Crime against Businesses: findings from the 2023 Commercial Victimisation Survey

vii. Home Office – Crime against Businesses: findings from the 2023 Commercial Victimisation Survey

viii. Home Office – The Economic and Social Costs of Crime, Second Edition

ix. British Retail Consortium - Crime Survey Report, 2025

x. Association of Convenience Stores – The Crime Report, 2025

xi. Department for Science, Innovation & Technology – Cyber security breaches survey 2025

xii. Department for Science, Innovation & Technology – Cyber security breaches survey 2025

xiii. Crime in England and Wales: year ending September 2025

xiv. Home Office – Crime against businesses: Commercial Victimisation Survey (CVS) update

xv. Home Office – Crime against businesses: Commercial Victimisation Survey (CVS) update

xvi. Home Office – Crime against Businesses: findings from the 2023 Commercial Victimisation Survey

xvii. Crime in England and Wales: year ending September 2025

xviii. National Crime Agency – National Crime Agency Annual Report and Accounts, 2024-2025

xix. National Crime Agency – Illicit Finance

British Chambers of Commerce | 65 Petty France, London, SW1H 9EU
britishchambers.org.uk | @britishchambers | 020 7654 5800