TACKLING BUSINESS CRIME: FSB MANIFESTO

Published: March 2016

@fsb_policy

fsb.org.uk

fsb
Experts in Business

fsb
Experts in Business

TACKLING BUSINESS CRIME: FSB MANIFESTO

"Average cost of crime to a small business now at £5,898"

1/3
small firms say crime is increasing

48%
of small businesses have been a victim of non-cyber crime

66%
of small businesses have been a victim of cyber crime

24%
of small businesses do not report crime

Reason for lack of crime reporting

46%
feel it would not achieve anything

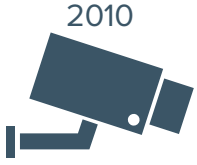
38%
do not trust police to find criminals

26%
say it's too time consuming

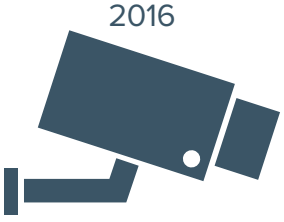
Smaller firms increase crime protection measures

Installed or upgraded a security system

25%
2010



41%
2016



80%
use computer security software

TACKLING BUSINESS CRIME

In May 2016, small business owners will have the opportunity to vote in the Police and Crime Commissioner (PCC) elections taking place in England and Wales. They will be looking to candidates to ensure that local police forces take tackling business crime seriously, have the resources from government to do so effectively. This manifesto explains how PCCs can do just that.

PRIORITISING BUSINESS CRIME

Business crime[1] affects all businesses. It is often the smaller firms who are hit the hardest because they cannot absorb the cost.

New FSB research reveals how smaller firms are being affected[2].

- 48 per cent victim – offline (non-cyber) crime
- 66 per cent victim – cyber crimes
- Three - average number of times FSB members have been a victim of offline crime
- Four - average number of times FSB members have been a victim of cyber-crime

Business crime has far ranging consequences beyond the direct financial cost of the loss or property damage. It can put insurance premiums up, damage a business's ability to meet customers needs, cause reputational damage with both customers and suppliers, negatively impact employees, jeopardise future work and waste valuable time.[3] A survey of FSB members found that:

- Average cost of offline crimes to FSB members is nearly £5,898
- Average cost of cyber crime to FSB members is nearly £2,976

Reducing business crime is fundamental to greater business prosperity. However, the extent to which crime against small businesses is prioritised by PCCs and local police forces varies by constabulary. Reducing the negative impact of crime against small businesses means placing business crime consistently at the heart of the anti-crime strategy of all PCCs.

Recommendations:

- Place business crime and the prevention of business crime, at the centre of your election campaign.
- Put business crime at the heart of future Police and Crime Plans. This should involve the development of a specific strategy to deal with business crime with clearly defined objectives, outcomes and measures of success. An example of this is the strategy developed for London by the Mayor's Office for Policing and Crime (MOPAC).
- Strategic prioritisation should be focused on the crimes that most impact small businesses. That means not just focussing on sophisticated crimes such as cyber and fraud but dealing effectively with the perennial problems of theft and anti-social behaviour. In our recent survey theft was experienced by a third of respondents.

1 'Business crime' is used in this manifesto as a term to describe both offline crime and cyber-crime perpetrated against businesses the owner(s) or their staff during the course of business'. For the purposes of this manifesto: 'cyber-crime' describes crimes that take place using networked information technology. This includes the new crimes which computers and associated devices have enabled and traditional crimes committed using ICT. 'Offline' or non-cyber crime describes traditional crimes i.e. committed in the physical world.

2 In January 2016 the FSB surveyed 1006 members on their perceptions and experiences of crime against their business, themselves and their employees (during the course of business) over the preceding 2 years (24 months).

3 Negative impacts on employees might include psychological trauma which requires an employee to take time off and get counselling.

RECORDING BUSINESS CRIME

In order to tackle business crime, the police need an idea of its scale and scope. The move to record incidents against businesses separately from other types of crime is essential to allocating resource to deal with business crime. The National Police Chiefs' Council (NPCC) has developed a specific definition of business crime, which all police forces are being encouraged to use. However, implementation is not comprehensive and uniform across England and Wales. In addition, too few businesses currently report incidents of crime. Business owners are fatalistic about the interest of the police in crime against business and the capacity of police forces to do much about it. Recent FSB research from small businesses revealed:

- 24 per cent do not report any crime against their business or staff
- 33 per cent only report the most serious crimes
- Only around one in five reported all the crimes their business and employees experienced

Many reasons were given by FSB members for this reluctance. However, the most frequently cited reason was a feeling that reporting the crime would not achieve anything (46%). Other reasons that were offered, included a perception that the police would not be able to find/ mount a successful prosecution of the perpetrators (38%), reporting a crime would be too time consuming (26%) and a; negative experience of previously reporting a crime to the police (21%).

Recommendations:

- Mandate the use of the new business crime definition by all constabularies. Produce clear guidelines about what qualifies as a business crime and what does not.
- Encourage small businesses to report every crime. Take measures to break down some of the negative perceptions such as by widely publicising how and where to report crime, making the process as easy and user-friendly as possible with minimum service user standards and seamless access to victim support services.
- Routinely conduct a comprehensive survey of local businesses on policing matters, akin to the 'Business Attitude Survey' in London, and use the data to improve the service provided to the small business community.
- Publish nationally comparable data on business crime in your area (reported and detected) to enable businesses to compare the performance of their local police with other forces.

WORKING WITH BUSINESS

In some areas the PCC and the police work effectively with local businesses. However, engagement by small firms across England and Wales is patchy. Our survey found low levels of engagement with the police:

- Only 6 per cent of smaller firms have met with or attended a meeting with their local Safer Neighbourhood Team and only 5 per cent have taken part in a Community Safety Partnership or a Business Crime Reduction Partnership.

Yet, the involvement of the local business community is essential in enabling a two way exchange of intelligence, information and best crime prevention practice between businesses and law enforcement agencies.

Recommendations:

- Act as an effective interface between the business community and the police.
- As part of the Crime Plan, devise and implement a strategy for increasing the regular interaction between the small business community and the local police force.
- Encourage more small business participation in local Business Crime Reduction Partnerships.
- Work with Local Enterprise Partnerships so that tackling business crime also becomes a key local economic priority.
- Use such partnerships to develop and exchange best practice towards tackling crime against business and disseminate the results to all small businesses in the area.
- Ensure small businesses are aware of and can use the Community Trigger[4] to ensure action is taken to address an anti-social behaviour problem.

4 The C ommunity Trigger' was introduced in the Anti-Social behaviour, Crime and Policing Act 2014.

CYBER CRIME AND FRAUD

Cyber-crime is a big threat to a small firms ability to fully exploit the benefits of the digital economy. Small firms rely more and more on online means to attract customers, sell products and run their businesses. As a result the threat of online crime and its consequences needs particular attention. The risk of cyber crime increases the costs of doing business and can even put a business out of action for periods of time. This can have devastating consequences for the ability of a business to serve their customers needs. FSB research found that the top three cyber-crimes experienced by FSB members were:

- Phishing attacks – 48 per cent
- Spear phishing attacks – 37 per cent
- Malware – 28 per cent (on the receiving end of at least one attack)

Recent reports by HMIC have identified a lack of local and regional capability among police forces to deal with cyber crime. There is an inconsistent patchwork of performance and standards of response and investigative capacity'[5]. Fraud and cyber crime have in many ways become synonymous. Fraud is also a significant and growing issue for small businesses. Nearly 10 per cent of FSB respondents to our business crime survey had been the victim of 'card-not-present' fraud.

Both fraud and cybe crime strike at the very heart of the business world, reducing levels of trust in commercial activity. The City of London Police have suggested, based on recorded incidents by the National Fraud Intelligence Bureau, that 70 per cent of fraud is committed online[6]. The existence of these crimes on a significant scale increases the cost of doing business for small businesses. The cost is not only the direct financial losses but includes indirect costs such as the negative impact on a business's reputation and associated reduction in customer confidence and trust. It can also result in higher costs for accessing vital small business services such as insurance, banking and loans. While many FSB members are taking basic preventative measures (80% are installing security software on their business ICT) many of the available cyber-security standards are failing to make an impact with FSB members (only 2% had taken up either ISO 27001 or the Government's Cyber Essentials Scheme).

Recommendations:

- Make cyber crime a priority for the local police force..
- Encourage national government to keep cyber crime and fraud at the top of the crime policy agenda and develop an effective national policing effort to tackle it.
- Work closely with government cyber-resilience initiatives such as the Cyber Essentials Scheme, Cyber Streetwise, Get Safe Online and business representative bodies such as the FSB to help inform and educate small businesses about the preventative steps needed to reduce the risk of cyber attacks.
- Encourage constabularies to significantly improve the support available to victims of cyber crime e.g. by training all frontline staff in how to more effectively handle incidences of such crime.
- Ensure that each constabulary has a cyber-investigation capability with the ability to leverage to get adequate funding and outside expertise when needed.
- Ensure constabularies take advantage of the planned improvements in the capabilities of the National Fraud Intelligence Bureau and Action Fraud to instigate a 'step change' in the identification, investigation and prosecution of fraud by prioritising fraud against business and investing in the capacity of their local force to investigate fraud.
- Improve partnership working between constabularies through:
  - Strengthening Regional Organised Crime Units (ROCUs) with more capability and capacity.
  - Supporting more inter-regional joint-working.
  - Contributing pro-actively towards ensuring a seamless and more effective nationwide exchange and analysis of intelligence on fraud and cyber crime against business.

5 HMIC (2014). 'The Strategic Policing Requirement: An inspection of the arrangements that police forces have in place to meet the Strategic Policing Requirement', can be accessed at: https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/2014/04/an-inspection-of-the-arrangements-that-police-forces-have-in-place-to-meet-the-strategic-policing-requirement.pdf HMIC (2015). 'Real lives, real crimes: A study of digital crime and policing', can be accessed at: https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

6 City of London (2014). 'Commissioner Speaks out on Cyber Security'.

7 A 2013 FSB report, found that around a third of respondents wanted a more robust police response to fraud. Source: FSB (2013), 'Online crime and fraud survey'.

fsb.org.uk

federationofsmallbusinesses

@fsb_policy

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

fsb
Experts in Business