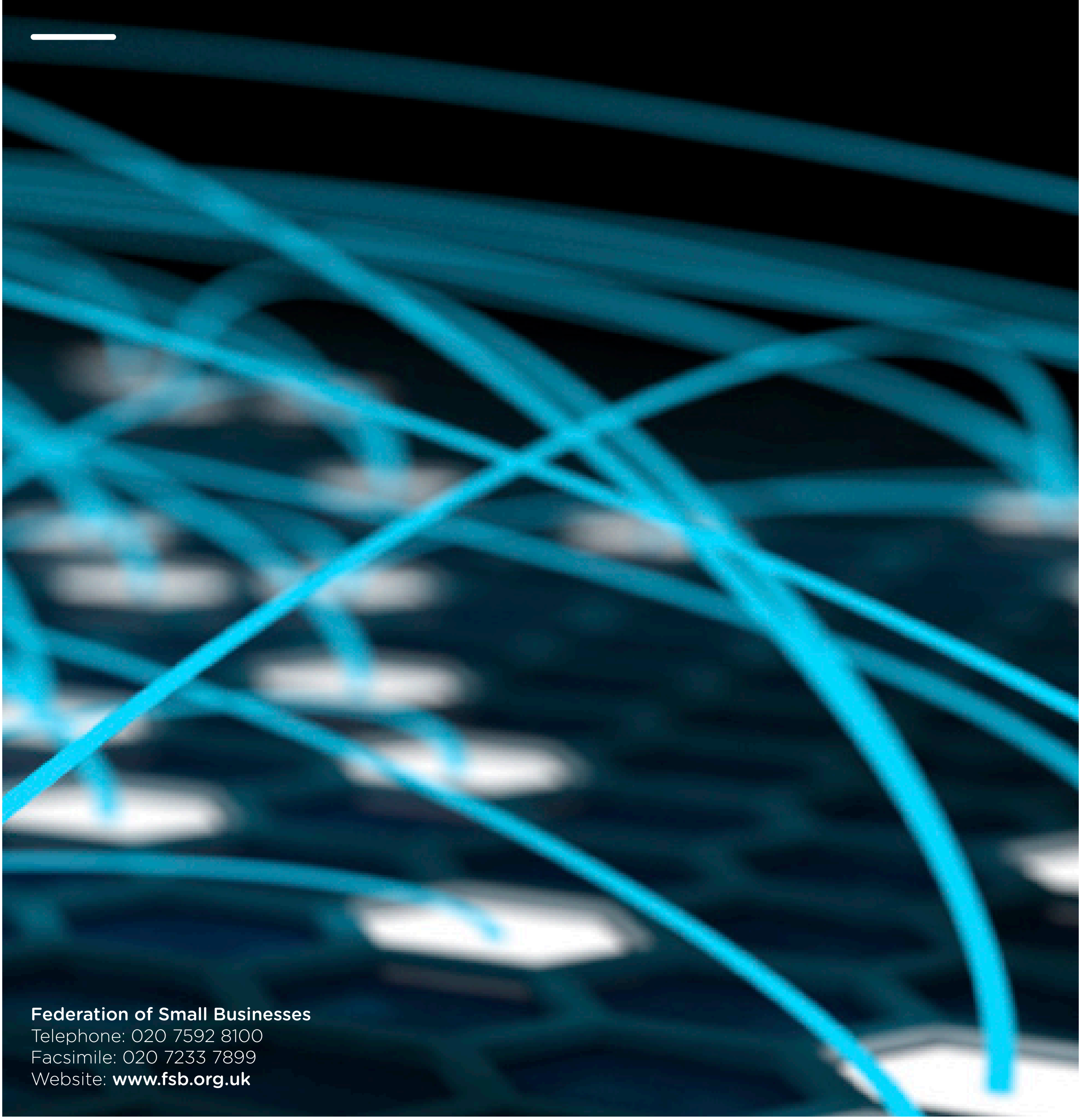
Federation of Small Businesses
The UK's Leading Business Organisation

Cyber security and fraud: The impact on small businesses



Federation of Small Businesses
Telephone: 020 7592 8100
Facsimile: 020 7233 7899
Website: **www.fsb.org.uk**

Contents

Authors:

Rosina Robson, Senior Policy Adviser

With:
Ann Swain, Home Affairs Chairman
Lee Campbell and David Springer, Home Affairs Committee

Joint Ministerial Foreword

James Brokenshire, MP
Parliamentary Under Secretary for Security
Home Office

Having personally been involved in the cyber security debate for several years now, I am pleased that the Home Office is working with the Federation of Small Businesses (FSB) to highlight the current experiences of small businesses.

Cyber security is a crucial part of the Government's National Cyber Security Strategy and we need to make sure that all businesses, large and small are engaged in implementing appropriate prevention measures in their business. This report will help give a greater understanding of how online security and fraud issues affect small businesses, giving guidance as well as valuable top tips to protect their business.

David Willetts, MP
Minister for Universities and Science
Department for Business, Innovation and Skills

The Department for Business, Innovation and Skills (BIS) published guidance in April 2013, *'Small businesses: what you need to know about cyber security'*, based on our comprehensive "10 Steps to Cyber Security" guidance. This guidance sets out the current risks, how to manage these, and plan implementation of appropriate security measures. We know only too well of the importance of securing buy-in from both big and small business in implementing appropriate protection against cyber risks - business success can depend on it. Increasing security drives growth.

I support all efforts, like the FSB's, to provide clarity on the issues small businesses are facing, and more importantly, what they can do about them. I urge all small businesses to follow the FSB's advice.

David Willetts

Foreword

Ann Swain, Home Affairs Chairman

The FSB is pleased to partner with BIS and the Home Office to bring you this report looking at the issues of fraud and online crime based on research and evidence from our 6,500 strong survey panel, including ways of tackling the problem.

The risk of fraud and online crime, both real and perceived, and the serious costs that can be involved are a clear barrier to growth for small businesses, costing each business up to £4,000 per year[1]. The recently published BIS guidance 'Small businesses: what you need to know about cyber security' sits alongside our simple Top 10 Tips to cyber security giving accessible and straightforward advice to small businesses, without the jargon.

Alongside the actions that Government and the public sector need to take, businesses need to help themselves more. Creating the link between business, regional business crime forums as well as the National Business Crime Forum, is important but this has to be reinforced with effective communication and managing the expectations of businesses, large and small. Effective partnerships with the banks, police and private sector is important if we are to counter this growing threat.

Essentially, the report investigates how an improved response to the issue of online crime and fraud should involve:

- Simplified and streamlined guidance targeted specifically to help small and micro businesses
- Building the capacity of law enforcement to respond to fraud and online crime
- Improving the response and guidance available from the banks and payment providers
- Boosting partnership working and information sharing within the private sector
- Ensuring businesses report all crime including online crime and fraud

We trust this paper will help inform the debate on cyber security.

[1] FSB 'Voice of Small Business' Survey Panel (September 2012)

Executive Summary

- Cyber security is a key focus of the National Security Strategy and estimates that **cyber crime costs the UK economy a significant £27 billion a year**. Small businesses have potential to drive economic growth through e-commerce but cyber crime is eating away at this potential. Despite the plethora of Government agencies and departments responding to the challenge, there are signs of progress in the improvement of support to small businesses in the form of Action Fraud.
- **FSB research gauges the average annual cost to small businesses of fraud and online crime at just under £4,000 per year**. Around three in 10 members have been a victim of fraud over the last year with the main three types of fraud experienced including; customer or client fraud (13%), card fraud including 'card not present' fraud (10%) and computer software fraud (6%). Small retailers particularly report the impact on their business of 'chargebacks' from card not present fraud transactions.
- **Around three in 10 members have been a victim of online crime over the last year**. Businesses have particularly had an issue with 'virus infections' (20%), 'hacking or electronic intrusions' (8%) or 'system security breach/loss of availability' (5%). The Payment Card Initiative Data Security Standard (PCI-DSS) presents issues for small and micro retailers being an international standard created for more complex big businesses rather than small business.
- **Two thirds of businesses have acted in some way to prevent fraud**. This includes 'regular installation of 'security patches' (36%), 'risk assessments' (20%) and 'staff training' (20%). Formal and written counter fraud policies and plans are less common. In terms of action to **minimise online crime**, four in five members have acted in some way including 'regular updates of virus scanning software' (59%), 'firewall' (47%) and, 'spam filtering software', (43%). Written formal information security plans and the introduction of information security standards are less common.
- In terms of **combating fraud**, businesses say that they are keen on the 'banks taking more responsibility' (45%) than is the case at present, particularly where card fraud is concerned. Businesses would also welcome a 'more effective police response' (31%) to fraud and 'more targeted advice and more effective signposting' (27%).

FSB recommendations

Businesses

- Seek out ways to protect your business from fraud and online crime using the FSB's 'Top 10 Tips', BIS guidance and resources available through Action Fraud and GetSafeOnline
- Report fraud to Action Fraud www.actionfraud.police.uk if it occurs and contribute to a more complete intelligence picture

Action Fraud

- Launch a national advertising campaign to build awareness of the Action Fraud reporting facility
- Make the Action Fraud website the main port of call for small business advice on prevention of online crime and fraud, effectively cross referencing to GetSafeOnline

Banks and card payment providers

- Make businesses aware of the importance of online security and the risks of fraud and the need to take preventative measures before they start trading
- Be more upfront with businesses about the risk of card not present fraud, making the message that 'authorisation doesn't guarantee payment' clear when businesses initially sign up for payment systems
- Streamline and simplify the PCI-DSS self assessment and compliance forms so they are more responsive to the needs of small and micro businesses

Police forces and PCCs

- Fully back and implement signposting to Action Fraud linking up effectively to give good advice and signposting to businesses at a local level
- Manage business expectations around the police response to fraud and online crime by highlighting the benefits of reporting in terms of feeding into a wider intelligence picture
- Inform businesses what the police do not have the capacity to deal with so they can take preventative measures to help themselves more

Private sector partnership

- Encourage the use of regional networks, such as the Regional Fraud and business crime forums, including the National Business Crime Forum, to promote consistent and concise advice on prevention to small businesses

FSB Top 10 Tips for businesses – Online Security

1. Implement a combination of security protection solutions (anti-virus, anti-spam, firewall/s)
2. Carry out regular security updates on all software and devices
3. Implement a resilient password policy (min. eight characters, change regularly)
4. Secure your wireless network
5. Implement clear and concise procedures for email, internet and mobile devices
6. Train staff in good security practices and consider employee background checks
7. Implement and test backup plans, information disposal and disaster recovery procedures
8. Carry out regular security risk assessments to identify important information and systems
9. Carry out regular security testing on your business website
10. Check provider credentials and contracts when using cloud services

Introduction

Fraud and online crime is a barrier to growth for small and micro businesses. It prevents some businesses from online trading because of the fear or actual risk of fraud. This is particularly concerning given that the Government is looking towards small businesses for economic growth and to create jobs. They also impose significant costs. Small businesses lose on average a significant £4,000 per year to fraud and online crime[2], an additional cost that they could well do without. This is an issue that can only be addressed through effective partnership working between businesses, Government and also the public and private sectors.

This report looks at the following areas:

- The current context to the cyber security debate and how small business policy and guidance sits within this
- The current experience of small businesses with regard to online crime and fraud and the associated cost to business, both in monetary terms and in management time
- Current actions taken by businesses themselves to mitigate the risk of fraud and online crime, and an evaluation of the current support and response framework

The focus of this report will be on the interests of small and micro businesses, rather than small and medium-sized enterprises (SMEs) as these businesses make up the vast majority of the small business community. The FSB is interested in targeted support to small and micro businesses in addition to evaluating how the current support and response network works for businesses of this size.

[2] FSB 'Voice of Small Business' Survey Panel (September 2012)

Definitions

Cyber crime:

The Association of Chief Police Officers' (ACPO) definition is: 'the use of networked computers or internet technology to commit or facilitate the commission of e-crime'. This is a broad definition capturing a range of crimes from espionage to those that target computer networks and devices to intellectual property theft.

Phishing:

The fraudulent practice of sending emails purporting to be from legitimate companies in order to induce individuals to reveal personal or sensitive business information e.g. credit card numbers, account information, PINs or passwords.

Spear phishing:

Involves individual targeted and personalized email messages to obtain sensitive information from a business or individual. The attacker has usually gained other business details in order to attempt to fish for more information.

Card not present (CNP) fraud:

Is the theft of genuine card details then used to make a purchase usually over the phone or internet (and the card is not present at the point of sale).

Bring Your Own Devices (BYOD):

Typically mobile devices owned by a user to access the business network and information. These devices may present serious risks to the business because they usually lack the required security solutions such as malware protection.

Malware:

Is 'malicious software' designed with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications or operating system. Examples of malware include viruses, trojans, keystroke loggers and spyware.

Network Access Control (NAC):

Is a form of security control to validate devices such as laptops, tablets workstations and smart phones requiring access to a network to ensure they are compliant with the security policies.

In the research, in order to keep the definitions straightforward, we refer to 'fraud and online crime' rather than cyber crime or e-crime which can be a remote term for some small businesses inferring a threat to national infrastructure. In some cases there will be overlap between the two areas i.e. that some, but not all fraud, is committed online.

Section 1: Current context to fraud and online crime risk and policy response

When the Government included cyber security as one of its top four national security challenges in 2010[3], it signaled a shift in resourcing and focus on meeting this continually growing and mutating challenge. A number of organisations have tried to gauge the cost of cyber crime to the UK economy over time and estimates vary between £18 billion[4] and £27 billion[5] a year. The National Fraud Authority (NFA) has published an Annual Fraud Indicator for the last three years signaling a cost of fraud at £45.5 billion to the private sector with £18.9 billion[6] specifically on SMEs[7].

Cyber crime is a clear barrier to growth for small businesses particularly considering the enormous growth potential in the future from e-commerce. Currently, two fifths (37%) of small businesses trade online, increasing from 33 per cent in 2011. Of those that trade online, 27 per cent claim this generates more than half of their business turnover. A further 20 per cent are actively considering trading online or plan to do so in the future.

The structures in Westminster and Whitehall co-ordinating the cyber security response have for some time been a myriad of different agencies with overlapping responsibilities including, for example; Home Office, BIS, Cabinet Office, Cyber Security Operations Centre (CSOC) and GCHQ, National Fraud Authority and NFIB (National Fraud Intelligence Bureau). SOCA (Serious Organised Crime Agency) is also morphing into the National Crime Agency with its new cyber crime unit coming on line in 2013. This picture has been given a certain amount of focus with the setting up of the Office for Cyber Security and Information Assurance (OSCIA) in the Cabinet Office providing strategic direction.

Importantly for the small business community, the NFA has set up Action Fraud[8] offering a single reporting centre for businesses and individuals, which the FSB called for in its last report on fraud and online crime[9]. The NFA leads the *Fighting Fraud Together* strategy[10] which is meant to be a genuine partnership between the relevant Government departments and agencies, the banks and the private sector signed by each organisation representing their buy in and commitment (FSB is a signatory). This is delivered through three strategic objectives: awareness, prevention and enforcement and is a step in the right direction, it will require sufficient resourcing to adequately deal with the problem.

[3] A strong Britain in an age of uncertainty: the National Security Strategy (2010)
[4] Detica and the Cabinet Office, The Cost of Cyber Crime, February 2011
[5] Cambridge University, Measuring the Cost of Cyber Crime, June 2012
[6] Annual Fraud Indicator, National Fraud Authority (March 2012)
[7] Note: revised figures for the AFI 2013 will be published in May 2013
[8] Action Fraud www.actionfraud.police.uk
[9] Inhibiting Enterprise: Fraud and online crime against small businesses, FSB (2009)
[10] www.gov.uk/government/uploads/system/uploads/attachment_data/file/118501/fighting-fraud-together.pdf

Wales have benefited for some years from positive partnership working arrangements with organisations such as e-crime Wales with an annual conference to discuss addressing the latest trends and threats. The Scottish Government has introduced a Cyber Minister and the Scottish Business Crime Centre is a positive initiative between the public and private sector providing advice, among other things, on online crime issues. The FSB Northern Ireland team has also been involved, through membership of the Business Crime Partnership and Organised Crime Task Force, in addressing the fraud and online crime challenge.

At a regional and local level, Regional Fraud Forums need to be joined up to the Regional Business Crime Forums, and in turn link to the National Business Crime Forum (NBCF) based in Nottinghamshire.

FSB members were asked why they do not currently trade online:

"Expensive credit card service machines very off putting"

"Strong concerns re card fraud and poor delivery services restricts online trading"

"Money laundering and cloning of my identity is a big problem and SOCA is unhelpful in bringing the fraudsters to justice"

"Too much bureaucracy such as self assessment PCI DSS forms and costs"

"Used eBay and PayPal and it's too expensive - impossible to make any money with their cost and rules"

"We have atrocious broadband speeds and it is acting as a barrier to development we are in a rural/remote location"

Section 2: Experience and costs of fraud and online crime

The following section looks at the current experience of, and cost to, small businesses with regard to fraud and online crime. In addition to cyber security issues it looks at payment security based on feedback and case studies from members on the issue of card not present (CNP) fraud and the impact of the PCI-DSS (Payment Card Initiative Data Security Standard).

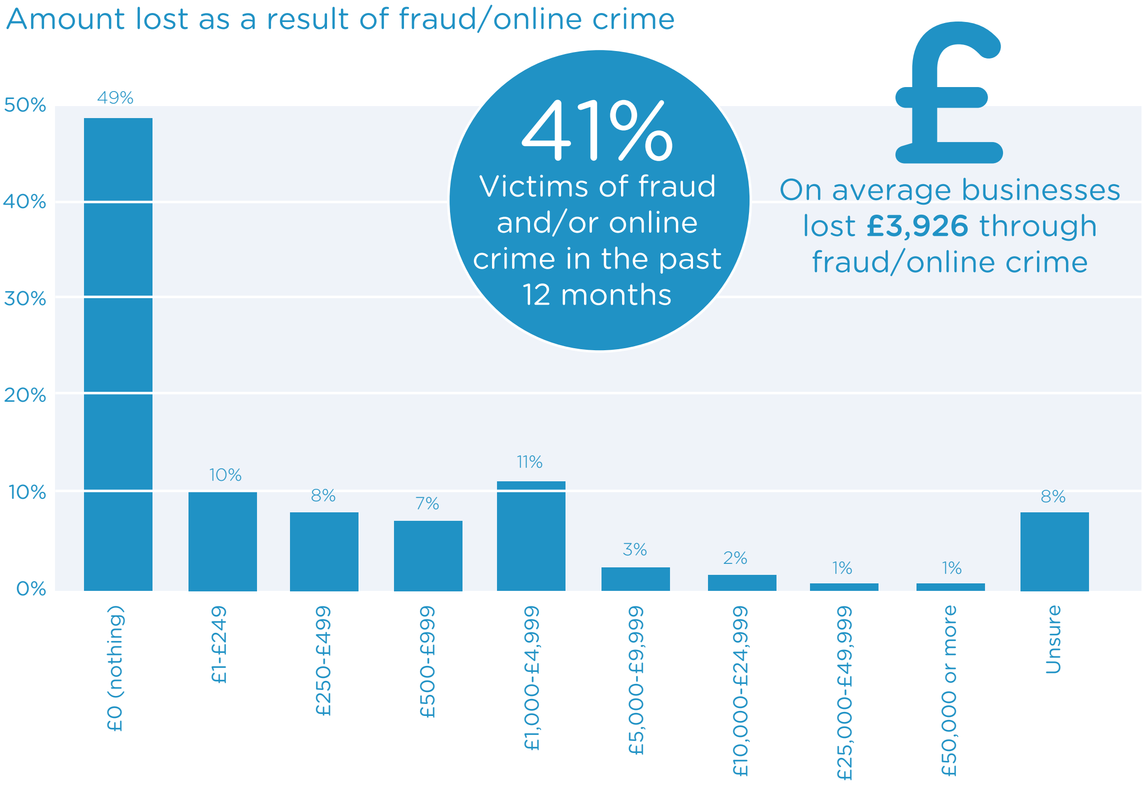
Costs to business

The cost of fraud and online crime is on average up to £4,000 per business per year and the cost to the wider economy even greater. The economy is also missing out from lost transactions from businesses that do not trade because they believe the security framework does not give them adequate protection. Some businesses report not wanting to trade online at all or opt instead to deal with UK customers only. In comparison, previous costs to business have been around £2,900 for fraud alone (not including the online crime element)[11]. The results also indicate that the types of fraud where larger sums of money are lost tend to be where members have experienced employee fraud and customer or client fraud.

How much money has your business lost as a result of fraud and/or online crime over the past 12 months?

Base: 1,105 (victim of fraud or online crime in the past 12 months)

Amount lost as a result of fraud/online crime



[11] FSB 'Voice of Small Business' Survey Panel (September 2010)

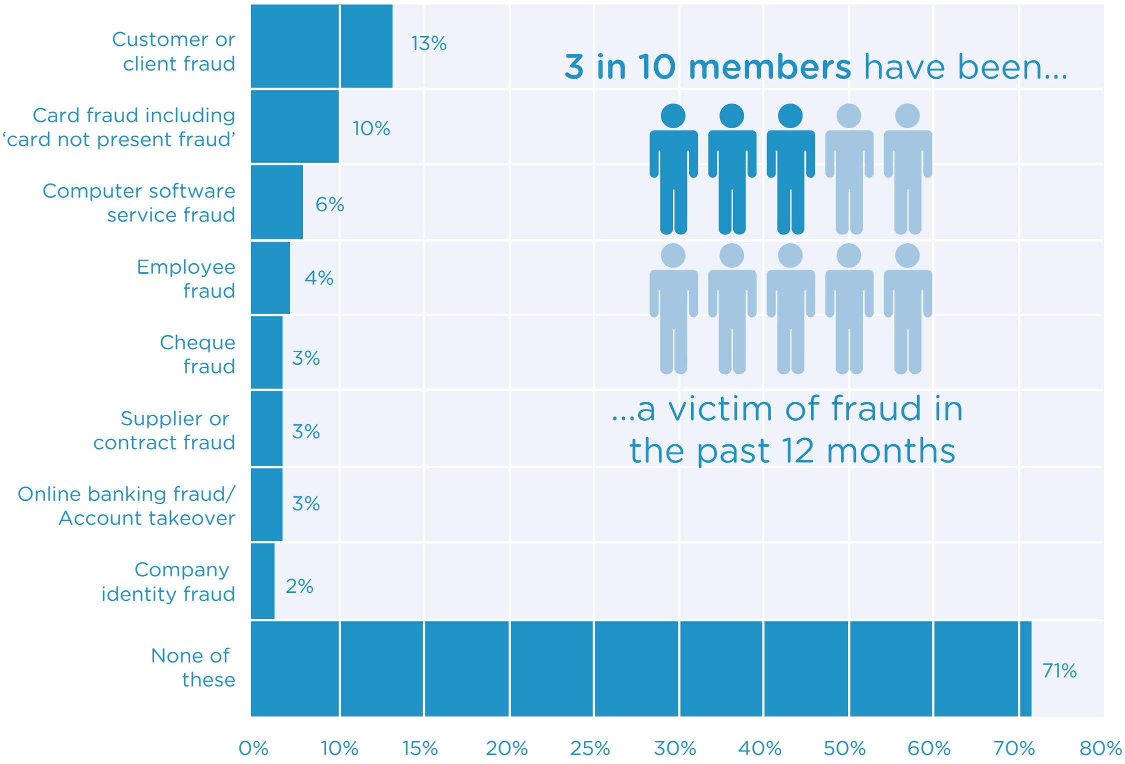
Experience of fraud

The FSB research[12] shows that around a third (30%) of members have been a victim of fraud over the last 12 months. This is clearly higher than previous FSB research in 2010, which indicated that figure was closer to a fifth (21%)[13] showing that the issue is on the rise. The top two member concerns remain the same with the new threat of computer software service fraud also coming into play[14]. It is important that straightforward guidance is available for small businesses to counter these threats and steps forward have been made by the NFA[15] in this regard.

Employee fraud is consistent with the results from 2010 and remains an underlying problem for small businesses. The FSB through its Legal Advice Line gives advice to members around carrying out adequate employment checks and carrying out regular business audits to help counter the issue[16]. Recent survey results from CIFAS (UK's Fraud Prevention Service) do show that employee fraud is actually on the rise[17]. Anecdotal evidence from members demonstrates that this type of fraud can be devastating for a small business when, for example, a trusted business partner or accountant siphons off a considerable sum of money from the business over a period of time.

Has your business been victim of any of the following types of fraud in the past 12 months?

Base: 2,596



[12] FSB 'Voice of Small Business' Survey Panel (September 2012)
[13] FSB 'Voice of Small Business' Survey Panel (September 2010)
[14] (Note: This was not highlighted as an option in the 2010 research).
[15] www.actionfraud.police.uk/resources-information-for-businesses
[16] See also: www.actionfraud.police.uk/small-businesses-know-your-employees
[17] Staff Fraudscape (April 2013) www.cifas.org.uk/staff_fraudscape_apr_thirteen

Businesses were asked about their current experience of fraud and flagged up a range of issues:

"Attempts to persuade us to register with meaningless trade marking registers"

"Bogus companies have tried to get us to supply"

"Claiming refund for missing items and non-delivery when signature showing proof of delivery has been received from Royal Mail"

"Companies ringing 'on behalf of' charities claiming our earlier agreement to pay for books/calendars/diaries promoting charities"

"Counterfeit banknotes"

"Increasingly, marketing companies are calling with the inference that they are from a large corporation. i.e. 'Hello it's Mike here with regards to your BT account''

Identity fraud

"Fraudsters use my name and then they make up my stationery and fake the signature. The document does not come from me and only if a company telephones me to authenticate it am I aware of the attempted fraud"

"People create websites with same name with a dot or dash, deliberately writing bad feedback or taking over adverts or trying to obtain access to online passwords"

Card not present fraud

Card not present (CNP) fraud remains a significant challenge for small businesses, particularly for retailers. Ten per cent of small businesses have been a victim of this type of fraud which rises to 16 per cent for retailers. Small businesses feel particularly bitter because they pay the banks and payment companies a charge for payment solutions yet there is no 100 per cent protection in return. Businesses can go through all the relevant checks yet still receive a 'chargeback' at the end of the process. This can happen where card details may have been cloned but not reported lost or stolen. Neither the consumer nor the bank pays. The business pays.

The FSB's concern for some time now has been that the banks and payment providers do not do enough to be upfront about these risks when businesses buy into security solutions. The message about 'authorisation doesn't guarantee payment' is lost in the small print and businesses have to foot the bill. The payment providers are not upfront about the risks and little advice is offered when the business initially signs up. One provider commented that they have moved away from providing written guidance for businesses and made it all available online[18]. This may work if a business already 'knows what they need to know', which is unlikely. Another issue arises where card issuer checks are slow to happen. In these cases, often the chargeback can happen three to six months after the actual event[19] when the business assumes the transaction has gone through. The business has lost the goods as well as the charge so they actually pay twice.

According to the UK Cards Association figures, card not present fraud decreased from 2008 through the recession, possibly due to the reduced number of transactions being made overall. However, in 2012 CNP fraud was on the rise again up 11 per cent to £245.8 million. Although the figures cannot be split by size of business, we suspect that small businesses often taking payment over the phone (rather than online) are bearing a proportion of these costs. To counteract the problem, 26 per cent of small businesses that have been a victim of card fraud are implementing 3D secure/online security systems[20] in their business. The issue is also that businesses are multiple victims, one member telling us he lost up to £9,000 from his kitchen equipment business over three separate chargebacks that brought his business to the brink a couple of years ago.

An FSB member and online clothing retailer gives us their experience of card not present fraud

Caron's business was victim to three chargebacks in succession a couple of years ago. She was surprised at the time that she only heard about these six to nine weeks after the event.

Caron says, "I've learnt a lot about payment security solutions available since the chargeback experience. I run my website/e-commerce from my own server and maintain it so that all patches are updated. I use a payment gateway and am fully PCI compliant. All these activities take a bit of time to set up and come at a price but are fundamental to running a secure business today.

The other problems that arise are with international orders where there is less information on cards and it's less easy and more expensive to check (payment gateways usually suggest on cards rated less securely that you ring the customer). The most secure action is not to fulfil the order, thus losing potential business".

[18] One example is: www.streamline.com/customer-zone/operating-instructions/merchant-operating-instructions-reducing-fraud/

[19] This is due to card scheme rules in response to EU Payment Services Regulations that protect the consumer more than the business

[20] Online security payment system such as Mastercard SecureCode or Verified by Visa

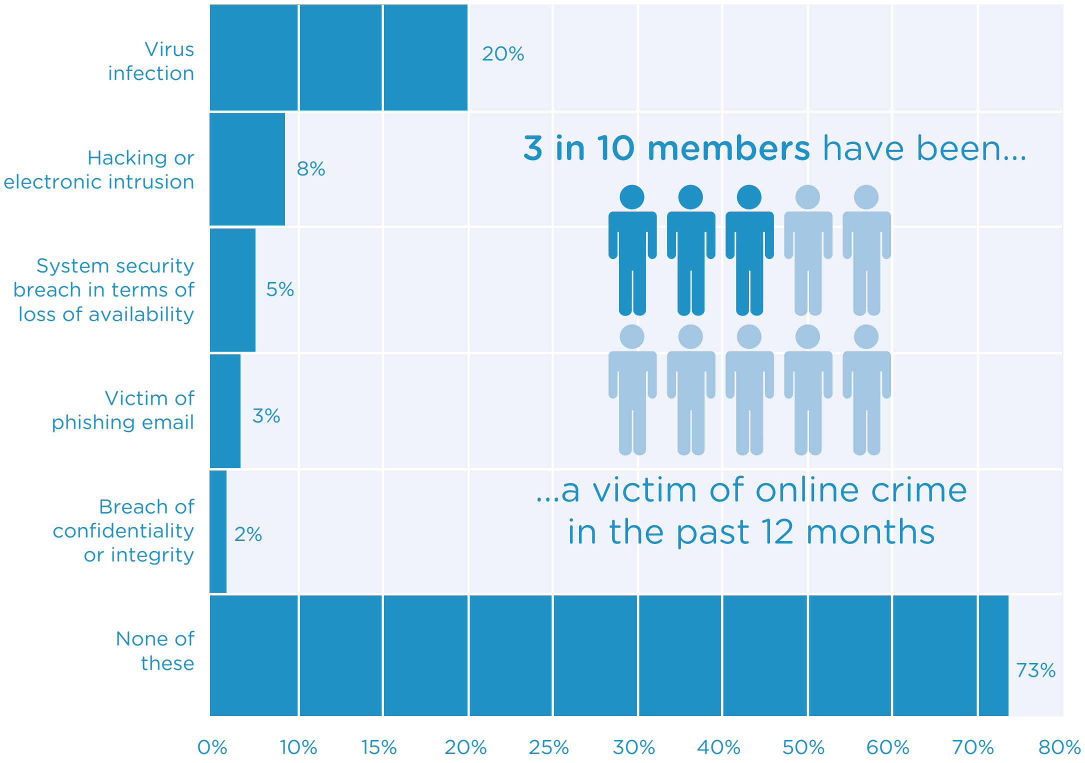
Experience of online crime

The research shows that around three in 10 members have been a victim of online crime over the last year. Businesses particularly have an issue with virus infections (20%), hacking or electronic intrusion (8%) or system security breach/loss of availability (5%). Concerning also is the fact that the vast majority of members feel they haven't been a victim (73%) but may not know that their system has been compromised or the victim of hacking or denial of service.

Compared with previous FSB research, businesses seem to be more aware of the risks of phishing[21] emails. An annual favourite is the phishing email to members reporting to be from HM Revenue and Customs about their tax return using some business information to try to tempt the business to enter further business details by return email. Even with slightly more sophisticated and targeted attacks (spear phishing) businesses have become more vigilant than was perhaps the case a few years ago. Businesses are thinking twice about the risks.

Has your business been victim of any of the following types of online crime in the past 12 months?

Base: 2,541



[21] The fraudulent practice of sending emails purporting to be from legitimate companies in order to induce individuals to reveal personal or sensitive business information

Businesses were asked about their experience of online crime:

“Virus, hacking, phishing and spyware attacks are blocked by our security infrastructure”

“Claim made that I requested and ordered advertising and attempt made to debit my bank account without authority”.

“eBay password hacked”

“Filtering out the phishing/scammers and clever virus distributors etc costs significant time and money”

“We have seen many attempts to log into our servers from the internet most being from China or Korea”

Bring Your Own Devices (BYOD)

Feedback from small businesses shows that BYOD presents additional risks to businesses. This is where employees bring personally owned mobile devices (laptops, tablets and smart phones) to their workplace and use these devices to access company information and applications. The main security concerns are malware infection to company data and systems, loss of data and unauthorized access. BYOD devices also increase IT costs in terms of extra security measures and resources to manage this additional risk. The use of encryption on company data, installation of mobile security solutions and Network Access Control (NAC) will help mitigate the risks. NAC will enforce security policies requiring the BYOD to comply with mandatory network security requirements, latest security updates and running anti-malware and firewall solutions for example.

PCI DSS – Payment Card Initiative Data Security Standard

Response from one small business to PCI-DSS compliance:

“I’m currently confused by my payment provider who is demanding that all businesses accepting card payments to be certified by a qualified security assessor and such certification be renewed annually - a further cost to business - £30 a year - desperate for micro businesses like ourselves. Making software fraud proof should be their responsibility and ours to ensure we adhere to their guidance”

PCI-DSS[22] is an internationally recognised data security standard that came into force over 10 years ago. It was created by the five major card schemes and was developed to help reduce card data theft and fraud. It applies to all businesses that take credit or debit cards, regardless of their size or transaction volume and businesses can be fined if they suffer a data breach.

Good data security is good business practice. However, FSB received complaints from members when the standard first came into force. Concerns centred on its impact on small businesses and the fact that the Standard was designed with big business, not small business, in mind. Small firms can either pay £1,000s to an assessor to comply with the standard or go through a lengthy self-assessment form that takes time and resources. The payment providers have taken some steps over recent years to improve and simplify these procedures but should go further. Streamline for example have a PCI online wizard tool to guide businesses through the process and claim that it only takes 30 minutes[23].

Member case study of PCI DSS

David Brown, Potters Crouch Candles Ltd
www.potterscrouchcandles.co.uk

“PCI DSS is THEFT – pure and simple. For a small business who use a single card machine connected to a secure telephone line, this is a money making piece of nonsense by the industry to take millions of pounds from small businesses. We pay two fees, one for our machine and one for online transactions, and then find out that in fact there is no proper security after all.

“We were recent victims of a card fraud to the tune of £950. There was no protection and we couldn’t claim any insurance as it is not insurable. We got no compensation and the payment provider still charged £20 or so for processing the fraudulent transaction because they ‘processed it in good faith and are still entitled to their fee.”

David commented that the payment provider had told him that they were aware of fraudsters targeting the types of products he was selling. They should share this information and make current risks available on their website. He also thinks that the payment provider could have been much clearer upfront about how the PCI-DSS applies to businesses with a single terminal and a phone line as this wasn’t clear and would have saved him time. He also suggested creating a compensation fund out of the revenue generated by PCI-DSS to refund even if in part those businesses that are victims of fraud.

[22] PCI Security Standards website: www.pcisecuritystandards.org.
[23] www.streamline.com/customer-zone/pcidss/

Section 3: Prevention measures and evaluation of current small business support network and solutions

This section looks at the steps that businesses have taken themselves to prevent online crime and fraud in the workplace outlined in Section 2. It also evaluates the current network of response and support to businesses for advice, prevention and enforcement.

Business action to prevent fraud and online crime

Fraud

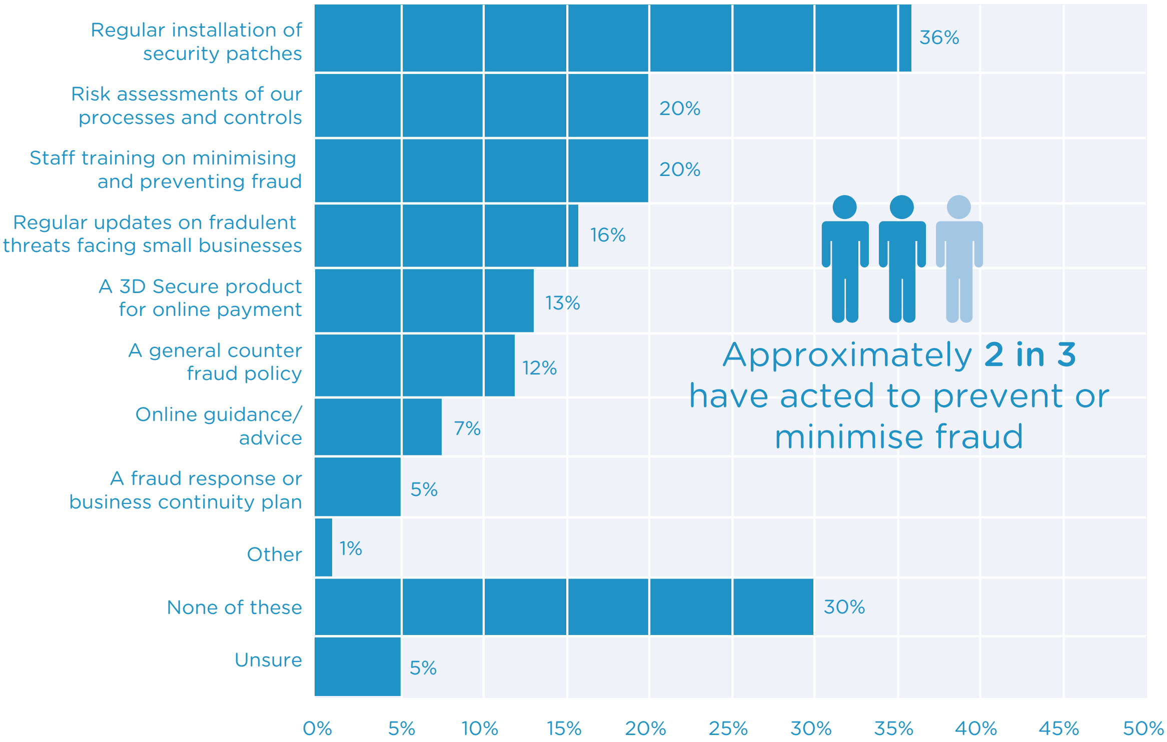
The majority of businesses are taking steps to prevent themselves from fraud and online crime. Two thirds have acted in some way to minimise their exposure to fraud. Of these over a third (36%) have installed security patches, carried out risk assessments (20%) or staff training (20%). Twenty eight per cent of retailers are also operating with 3D secure.

Businesses are less likely to opt for written processes and procedures such as a fraud policy (12%) or a fraud response or continuity plan (5%), largely because the majority of members are smaller, micro businesses and this type of response involving documenting procedures can be less appropriate. Worryingly, a third of businesses have not taken any action at all to combat fraud.

Which of the following, if any, have you sought or introduced into your business to help prevent or minimise your exposure to fraud?

Base: 2,578

Actions used to prevent or minimise fraud

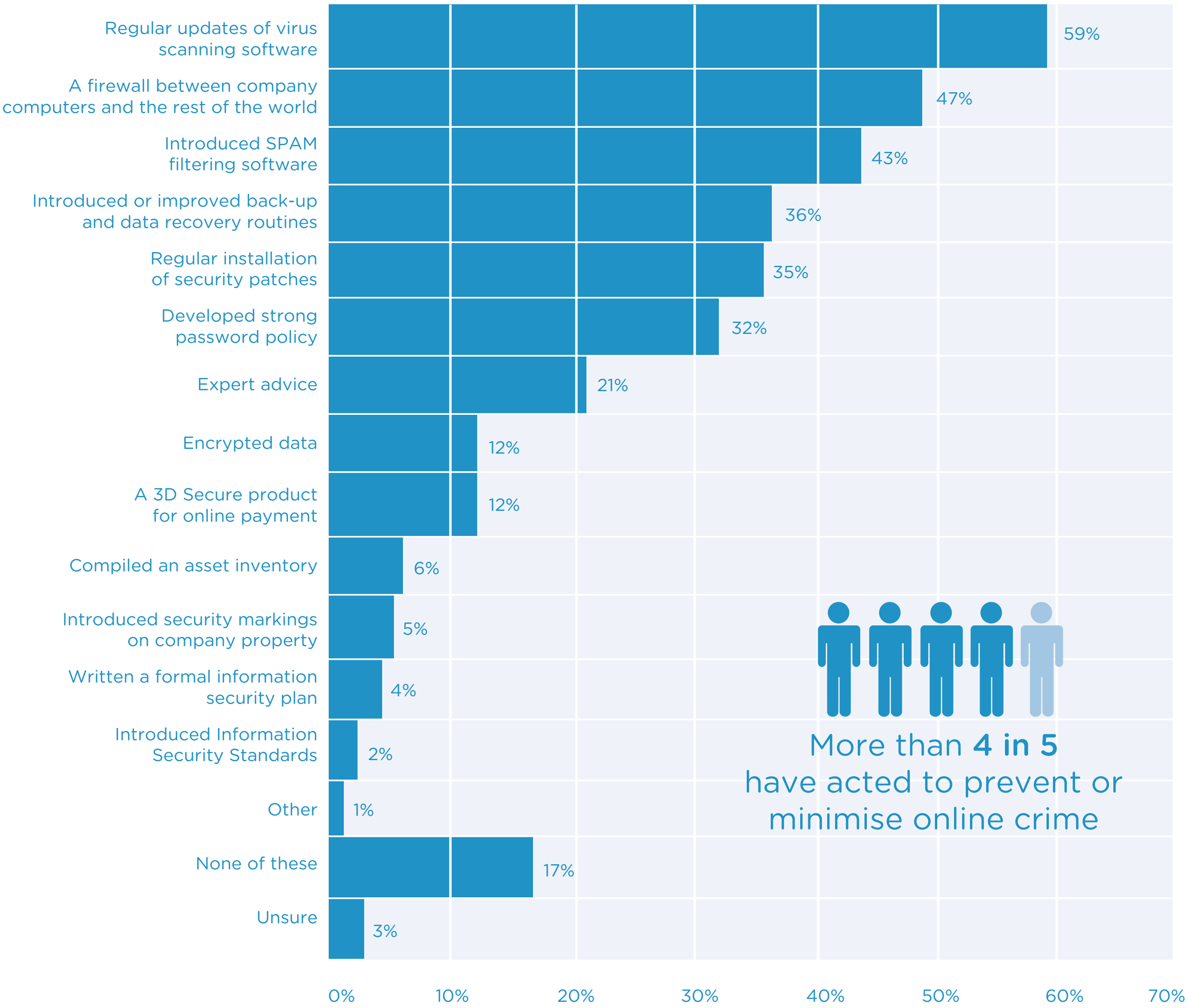


Online crime

More than four in five businesses have acted to prevent their exposure to online crime risks. It therefore appears that the majority of small businesses are getting the basics right in terms of introducing regular updates of virus scanning software (59%), a firewall (47%) and spam filtering software (43%). A fifth (21%) have opted for taking expert advice from an information security professional. Again, as with fraud, very few businesses have implemented written policies or procedures such as a formal information security plan (4%) or information security standards (2%). Seventeen per cent have taken no action at all to protect the business against online crime.

Which of the following, if any, have you sought or introduced to help prevent or minimise your exposure to online crime?
Base: 2,580

Actions used to prevent or minimise online crime



More than **4 in 5** have acted to prevent or minimise online crime

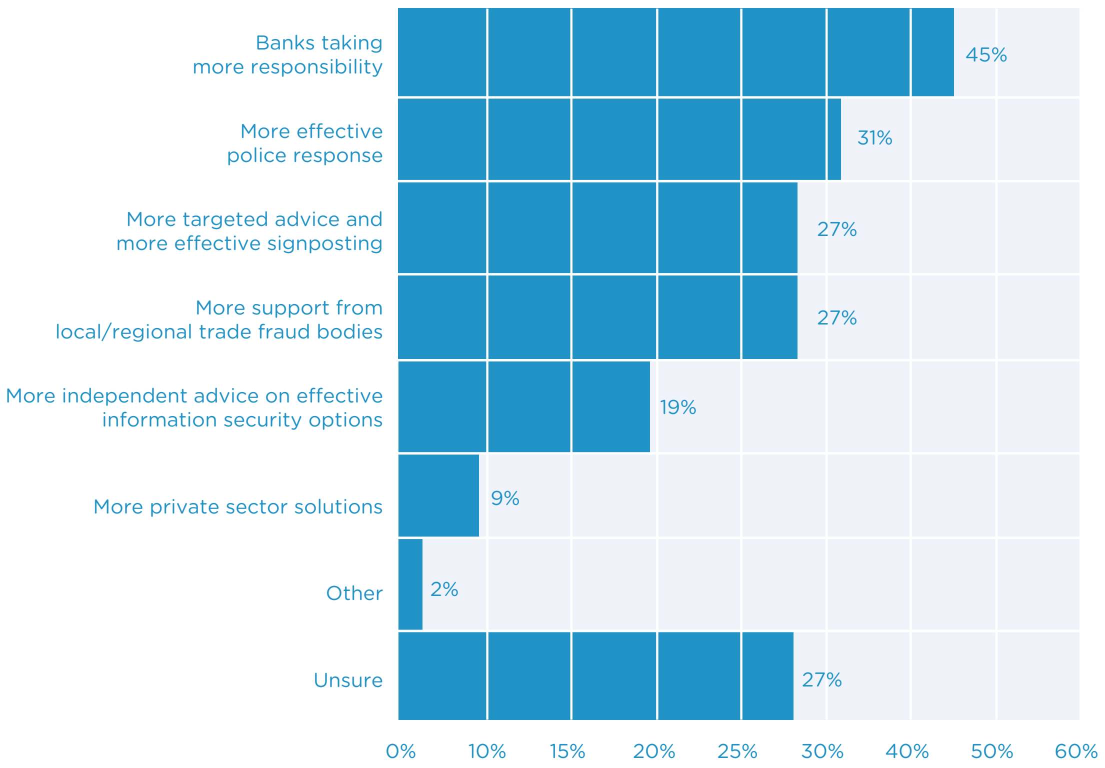
Measures to combat fraud

In terms of action to combat fraud, businesses believe that the banks should take more responsibility (45%) particularly in cases of card fraud, a view held particularly strongly by the retail sector. Businesses also see that a 'more effective police response' (31%) would be useful and more targeted advice and effective signposting (27%). FSB supports continued funding to the e-crime unit to become part of the NCA, giving specialist expertise in cases of organised and international fraud and cyber crime. Businesses also comment that they are not sure how to access reliable independent advice for relevant information security options for their business. The key here is to promote those sources that have formal accreditations for example to the British Computer Society and British Institute of Engineering and Technology.

What more could be done to help small businesses combat fraud?

Base: 2,538

Suggestions to combat fraud



Businesses were asked what would be useful from their point of view in terms of combating fraud and online crime:

"Free banking for card transactions for startups - Bank costs are prohibitive if all you want to do is experiment and make a few sales of a few £10 / £100 each before launching a big sales drive"

"Better legal safeguards for small amounts of money (bounced cheques, refusal to pay etc)"

"Encourage ISPs and wholesale ISPs to introduce more effective measures to detect and prevent online attacks at source rather than relying on end-user protection. Change in policy in UK to allow tracing and elimination of international threats at source, particularly phone and mail"

Current support framework

There is a complex matrix of Government departments and agencies tasked with taking on the fraud and online crime challenge. The picture in terms of available guidance to business is improving with the roll out of Action Fraud around the country. However, anecdotal evidence tells us that awareness levels of GetSafeOnline.org and Action Fraud as a reporting centre and source of advice is still very low among the business community. The need for a public awareness raising campaign is addressed by the National Audit Office (NAO) and the FSB supports this[24].

The National Fraud Authority (NFA) has gone some way to address this through an SME segmentation research and analysis project. This has put them in a position to now target specific groups of SMEs with a specific message around fraud advice and prevention. Through the funding attached to the UK's Cyber Security Strategy, the FSB feels resources should be maintained to enable business support and guidance on counter fraud measures through Action Fraud, the NFA and recent positive initiatives through guidance from BIS. A co-ordinated approach with cross referencing to different sources of guidance and materials needs to take place.

The FSB has been monitoring the cyber security debate in Europe including the recent publication of the Cyber Security Strategy[25] and Directive on information security obliging companies to have IT security mechanisms in place. There are compliance costs attached to small businesses for this although it appears from the initial draft that micro businesses may be exempted from some measures so as to not impose a disproportionate burden. The FSB will also continue to work with Nominet around work with law enforcement to ensure that rogue websites or operators are shut down promptly whilst putting in place safeguards to protect legitimate businesses.

[24] The UK cyber security strategy: Landscape review, National Audit Office (February 2013)

[25] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Insurance industry

Businesses comment that there is no insurance cover available for scenarios where card not present fraud chargebacks happen. However, there are a number of products available to counter the growing cyber threat and the industry believes that not enough businesses are taking advantage of these[26]. The FSB's own insurance brokers, and other providers signpost members to a CyberProtect product providing cover for investigation and recovery costs when they suffer loss of data or misuse of their computer or IT equipment. In order to secure these types of products the Financial Conduct Authority (FCA) demands that businesses in the financial services sector both have a risk assessment in place and procedures to mitigate fraud, especially money laundering. All small businesses should look into finding appropriate cover for their businesses both considering internal and external risks.

Banks and payment providers

Issues with the banks, particularly around card not present fraud and the PCI-DSS, have already been identified. There is wider work to be done by the industry to collaborate in producing integrated and simplified security products and solutions that are easily understood and meet business' payment security needs. The FSB would like to see the industry look again at solutions for increased security particularly with payments taken over the phone (e.g. dynamic passcode authentication) that was considered a few years ago. One issue is banking infrastructure which is often assumed to be more advanced than is actually the case[27]. Addressing some of the frailties in existing infrastructure by improving the availability of data on customers and transactions and improving information sharing between institutions will help the banks reduce the incidence of fraudulent activity too. There is also a recognition by some payment providers that the expertise around fraud risks to business could be improved through training in bank branches at a more local level.

Police forces and Police and Crime Commissioners

The police response to fraud and online crime is developing; it is only at the start of the process and needs to go further. The Police Central e-crime unit has trebled in size and developed a framework for cyber specials (volunteer police officers with specialist cyber skills)[28].

The FSB has been tracking the roll out of Action Fraud to police forces around the country over the last few months. This process is now complete and essentially means that when individuals and small businesses report fraud to the police they will be signposted to Action Fraud. Forces should spread the word internally but also do an awareness raising drive with the public and businesses at a local level. Action Fraud will take the crime report and gather the intelligence centrally, which has not happened to date. Targeted investigation packages will be developed for individual forces and the NCA to pursue.

[26] Cyber market is sluggish despite increased attack, Insurance Times (April 2013)
[27] Financial infrastructure: can banks afford not to change? Intellect (February 2013)
[28] The UK cyber security strategy: Landscape review, National Audit Office (February 2013)

It is important that the police help in the process of managing business expectations around the response they can expect in fraud cases. For instance, the police will now only respond to fraud where there is an immediate need to respond. This new roll out although positive in some respects, allowing a greater intelligence picture, is unlikely to improve the response for small businesses that are victim to individual frauds to the tune of £1,000s each time. This has a direct impact on their business but on the wider economy too given the high volume of smaller frauds.

Elected Police and Crime Commissioners have a clear role to play in reducing online crime and fraud. Cyber security is included as a 'strategic policing requirement'[29] as an area that forces must deliver on, but will not necessarily be under pressure from the public to address. We encourage individual forces to work together with the e-crime Unit and other forces to improve the reporting and prevention of online fraud whilst responding promptly to other forms of fraud.

Despite the introduction of PCCs encouraging forces to work to their own individual police and crime plans, forces must look to working together. The Met Police on e-crime and the City of London Police as the lead force on fraud, in addition to signposting to Action Fraud, have an important role to play in training and building the capacity of forces around the country to deal with fraud and online crime.

International Security Standards

Businesses have made clear their views on the PCI-DSS but there are also a range of other international security standards available to businesses too, such as ISO/IEC 27001[30] and PAS 555. As already set out, small and micro businesses do not opt naturally for complex processes and procedures suggested by some of these standards. Some have costs and procedures attached in achieving the standard which may be more suitable for some small or micro businesses than others. BIS is consulting with industry to investigate the value of current standards and devise a preferred Industry standard in this area for Government to use. Worryingly for small businesses, despite the work going on in Government to reduce red tape around the public procurement process, the plan is to use this standard as an obligatory part of this. The FSB would prefer that any attempt to link information security to procurement is carried out through a risk based approach.

Regional networks and partnership working

There are some useful regional and local initiatives such as the Regional Fraud Forums and a national umbrella group that co-ordinates the work. These forums foster useful partnership working, information exchange and events particularly between big and small business and the public sector. The FSB is a signatory to the Fighting Fraud Together strategy led by the NFA and we support this partnership approach to information sharing both within the private sector and the public sector as well.

[29] The Strategic Policing Requirement, Home Office (July 2012) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/117445/strategic-policing-requirement.pdf

[30] http://www.bsigroup.co.uk/en-GB/iso-27001-information-security/ISO-27001-for-SMEs/ http://www.bsigroup.co.uk/Documents/iso-27001/resources/BSI-ISOIEC27001-Assessment-Checklist-UK-EN.pdf

Conclusions

As this paper has demonstrated, online crime and fraud is a growing and a real threat for small businesses. It is a continually mutating challenge and businesses need to be live to the many different types of frauds to which they may be victim, in addition to cyber security issues where they may not even know their system has been compromised.

The fact that each small business loses up to £4,000 per year to fraud and online crime should be a wake-up call also to those who have not so far implemented protections in their business. Research has shown that the majority of FSB members are getting the basics right in terms of protections. The FSB will continue to work with the NFA, Fraud Advisory Panel, BIS and other groups to signpost effective counter fraud and online crime guidance to members. Equally the banks and payment providers should improve their communications with businesses around the risks in addition to Government leading an awareness raising campaign to promote Action Fraud to businesses. Police forces have an important role to play at a local level in signposting businesses to reporting and advice on prevention through Action Fraud as well, and to highlight how businesses should report on this crime.

Method

The research findings analysed in this report are based on a survey of the FSB 'Voice of Small Business' Survey Panel which is broadly representative of the wider FSB membership. The fieldwork took place between 20 September and 3 October 2012. All panel members were invited to take part (6,432) with responses from 2,667 members, a 41 per cent response rate. The survey was designed and hosted by Research by Design Ltd on behalf of the FSB.

Useful links and advice for small businesses

Action Fraud – the UK's national fraud and online crime reporting centre
www.actionfraud.police.uk
www.actionfraud.police.uk/small-businesses-know-your-business (small business toolkit)

Get Safe Online
www.getsafeonline.org

Department for Business
Small businesses: what you need to know about cyber security
www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know

Fraud Advisory Panel
www.fraudadvisorypanel.org
www.fraudadvisorypanel.org/pdf_show_169.pdf (FSB cloud computing factsheet)

Bank Safe Online
www.banksafeonline.org.uk

Keep your domain name safe
www.agreatplacetobe.co.uk/keepyourdomainsafe

PCI Security Standards
www.pcisecuritystandards.org/documents/pci_ssc_quick_guide.pdf

Card not present fraud guidance
www.theukcardsassociation.org.uk/cards-transactions/card-not-present.asp
www.financialfraudaction.org.uk/Retailer-payment-authentication.asp
www.financialfraudaction.org.uk/Financial-cnp-fraud.asp

Scottish Business Crime Centre
www.sbcc.org.uk

e-Crime Scotland
www.ecrimescotland.org.uk

e-Crime Wales
www.ecrimewales.com

Northern Ireland
www.nibusinessinfo.co.uk/content/security-and-crime-prevention