SMALL BUSINESS REPUTATION & THE CYBER RISK

KPMG

BECYBERSTREETWISE.COM

Executive summary

In the past few years there has been a rapid expansion in the development and adoption of new communications technologies which continue to transform Government, business and the ways in which we interact with each other. Cyber crime undermines confidence in our communications technology and online economy. There were an estimated 5.1m incidents of fraud and 2.5m incidents falling under the Computer Misuse Act recorded last year (ONS, 2015).[1] Add in recent high profile hacking cases and the issue of cyber security is now more important than ever.

But is it front of mind for small businesses? Cyber Streetwise and KPMG surveyed 1,000 small businesses and 1,000 consumers across the UK to assess how small businesses feel about cyber security, how they are protecting themselves and the impact of a cyber breach on their reputation.

KEY POINTS

Cyber security was cited as one of their top concerns by less than a quarter of small businesses

23%

yet it is fast becoming the only way to do business:

83%

of consumers surveyed are concerned about which businesses have access to their data and

58%

said that a breach would discourage them from using a business in the future.

Recently published KPMG Supply Chain research supports this;[2]

94%

of procurement managers say that cyber security standards are important when awarding a project to an SME supplier and

86%

would consider removing a supplier from their roster due to a breach.

UK small businesses value their reputation as one of their key assets. Yet they are hugely underestimating the likelihood of a cyber breach happening to them and its long term impact:

60%

of small businesses surveyed have experienced a cyber breach, but only

29%

of those who haven't experienced a breach cited potential reputational damage as an 'important' consideration.

The impact of a cyber breach can be huge and long lasting.

89%

of the small businesses surveyed who have experienced a breach said it impacted on their reputation. Those who experienced a breach said the attack led to:

31% Brand damage

30% Loss of clients

29% Ability to win new business

Quality of service is also a risk. Those surveyed who experienced a cyber breach found it caused customer delays

26%

and impacted the business' ability to operate

93%

So what do these findings mean for small businesses?

What's clear is that protecting business' data not only helps secure reputation, but puts small businesses in a strong and competitive position to offer the service that customers now expect.

Companies failing to adequately protect their data from cyber breaches don't just put a few documents at risk. Losing valuable data can have a lasting and devastating impact on a company's finances, customer base, ability to grow – and ultimately its reputation.

Adequate cyber security does not need to be time consuming or complex. Businesses should follow these three simple steps: use three random words to create a strong password, install security software on all devices and always download the latest software updates.

[1] These are results from an ONS field trial, carried out for the first time in 2015, of new survey questions on fraud and cyber-crime as part of the Crime Survey for England and Wales. It should be noted that these capture incidents which may not meet the threshold of a crime under the Home Office Counting Rules. http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html

[2] SME Supply Chain, KPMG, 2015

Many small businesses are unprepared and unconcerned when it comes to cyber breaches; but customers are increasingly concerned about the security of their personal data.

48% of London consumers surveyed say they are 'extremely concerned' about having their personal details stolen

6% of London small businesses surveyed say they have no online security measures in place

THE CYBER MYTH

It won't happen to us...

Half of small businesses (51%) surveyed think it's unlikely or very unlikely that they'd be a target for an attack, which perhaps helps to explain why only a third feel 'completely prepared' for a cyber security breach (33%).

What's more, **68%** of those small businesses surveyed who have never been a victim of a cyber breach think there is **little to no risk** of them becoming one.

THE REALITY

Six in ten of the small businesses surveyed have previously experienced a breach (599), and over half of those were in the last year (63%). However, only a quarter of small businesses (23%) say that it is one of the things that concerns them the most as a business owner.

But almost **two thirds of consumers** (64%) surveyed think that there will be more cyber attacks this year. This attitude gap should be a note of caution for small companies.

The majority of consumers (83%) surveyed are concerned about which businesses have access to their data and whether it's safe. Nine in 10 consumers (90%) admit that hearing about security breaches in the news, or from friends and family, makes them concerned about the security of their information. This puts clear pressure on small businesses to take action in order to reassure customers that their details are secure.

It's not just consumers that are applying this pressure. A recently published KPMG survey of 175 procurement managers highlights that an overwhelming **94% believe that cyber security standards are important when awarding a project to an SME supplier.**[3]

Although the vast majority of small businesses surveyed have at least one digital security measure in place, just half use security software (such as anti-virus); and only 52% have a strong password policy and regularly update software. However, small businesses still need to do more to protect themselves from cyber threats. Worryingly, **one in ten** (11%) surveyed admit that they haven't taken any steps to protect their data.

So what does this mean for small businesses?

As a top target for hackers and customers truly concerned about the safety of their data, small businesses are at risk of losing customers, or their supply chain, if they don't have adequate protection in place.

The regional snapshot

Compared to other regions, consumers surveyed who were based in **London** were the most worried about having their personal details stolen – **48%** say they are 'extremely concerned'. The London small businesses surveyed were also the most vulnerable compared to other regions, with 6% admitting they have no online security measures in place – twice the number than the national average (3%).[4]

The sector snapshot

The **design and creative** industries surveyed were the least concerned about cyber security compared with other sectors - **11%** admit that they are not prepared for an attack but it is not a concern. **Manufacturing** small businesses feel most prepared for an issue – 40% say they are completely prepared, sitting higher than the national average of 33%.[5]

Those in the **retail** industry are leaving their data most exposed according to the survey, with **one in seven** (14%) saying they haven't taken steps to protect their data. This is compared to the national average of 11%, and 9% for both the financial services and creative industries.[6]

40% of small manufacturing businesses surveyed say they are completely prepared for a cyber issue

1 in 7 small retail businesses surveyed haven't taken steps to protect their data

[3] % SME Supply Chain Research, KPMG, 2015
[4] % are out of a consumer and small business respondent base by region of 100
[5] % are out of a small business respondent base by sector of 200
[6] Base figures: retail – 25 (14%), financial services – 18 (9%), Design – 17 (9%), national average – 108 (11%)

Small businesses are putting themselves at huge risk by underestimating the big impact a cyber attack can have on their reputation.

37%
of small businesses surveyed in Wales say market reputation is a top three business worry

THE CYBER MYTH
A cyber attack won't affect our reputation

Despite the **vast majority** of small businesses (93%) surveyed thinking about their reputation frequently, or indeed all the time, they aren't considering how a cyber breach could affect it. In fact, 29% of small companies surveyed that haven't experienced a breach say the potential damage a cyber breach could cause is an "important" consideration.[7]

Less than half of these small businesses (46%) think that a cyber breach would discourage customers from using them in the future, and only a third (37%) of those surveyed would definitely expect a supply chain customer to vet their cyber security.

THE REALITY

In reality, **small businesses are underestimating the true impact that can stem from a breach**. The majority of consumers (**58%**) surveyed said that a breach would discourage them from using a business in the future. This is supported by recent KPMG Supply Chain research which shows a huge **86%** of procurement departments would consider removing a supplier from their roster due to a cyber breach.

Of the 599 small businesses who experienced a cyber breach, the **majority (89%) felt the attack impacted their reputation**.

The breach took an average of 26 hours to resolve for small businesses, which is a large chunk of time to stop running your company to deal with an issue – not to mention the costs incurred and it being all too obvious to your customers.

Small businesses who have encountered a breach said it caused the following reputational damage:[8]

- Brand damage (31%)
- Loss of clients (30%)
- Ability to attract new employees (30%)
- Ability to win new business (29%)

With 27% reporting that customers were angry about the cyber breach and a quarter saying that customers lost trust in the business, it's perhaps no surprise to hear that this dissatisfaction spreads through word of mouth. A quarter of the businesses that encountered a cyber breach said they received **negative reviews on social media (25%)** and **negative coverage in the media (24%).**[9]

The regional snapshot

Compared to other regions, small businesses surveyed who were based in **Wales** were the most concerned with their market reputation, with **nearly two in five** (37%) saying it's a top three worry. In contrast, nationally, small businesses rank the top three worries facing their business as maintaining product quality (39%), maintaining cash flow (36%) and competition within the market (34%).[10]

[7] 38% of small businesses surveyed that haven't experienced a breach said that the potential damage to their business's reputation by a cyber security breach was of "consideration and some importance"

[8] Base figures: brand damage - 185 (31%), loss of clients – 181 (30%), ability to attract new employees – 179 (30%), ability to win new business – 176 (29%)

[9] Base figures: negative reviews on social media – 149 (25%), negative coverage in the media – 143 (24%)

[10] % are out of a small business respondent base by region of 100

Small businesses are putting themselves at huge risk by underestimating the big impact a cyber attack can have on their reputation. Continued

THE REALITY Continued

Quality of service is also at risk. Those who experienced a cyber breach found that it caused customer delays (26%) and **impacted the business' ability to operate (93%)**. For example, a fifth (21%) of small businesses had to take their website offline, nearly a third (32%) had to pay someone to help fix the issue and a fifth (20%) incurred legal costs[11].

It's not just external word of mouth that is damaging to a small business' reputation, the majority of businesses (93%) also said that the cyber breach impacted their employees; causing stress and concern (29%) and/or worry about the loss of their personal data (27%)[12].

For the small businesses who have experienced a breach, the impact has been long lasting. Since being attacked, more than **one in four (26%) have been unable to grow in line with previous expectations**, and almost a third (31%) said it took over six months for the business to get back on track[13].

39%
of small businesses in financial services that have experienced a breach say they lost customers as a result

31%
of small manufacturing businesses that have experienced a breach said it affected their ability to win new business

So what does this mean for small businesses?

Now more than ever it is essential for small businesses to take action to protect themselves from cyber threats. Without adequate protection they are risking their future business growth and development. Having measures in place to be cyber secure is fast becoming the only, and expected, way to do business.

The sector snapshot

Compared to other sectors, two fifths of small businesses surveyed in **manufacturing** that experienced a breach said it has affected their **ability to attract new employees (41%)** and the **ability to win new business (31%)**, compared to 30% and 29% nationally. A quarter of those surveyed in **retail** felt it impacted their ability to attract new people and 21% said it affected new business.

Financial Services as an industry is most likely to lose customers as a result of a cyber breach with nearly two in five businesses (39%) surveyed seeing customers leave, compared to 30% nationally.[14]

[11] Base figures: customer delays – 154 (26%), website offline – 127 (21%), pay someone to fix the issue – 193 (32%), incurring legal costs – 122 (20%)

[12] Base figures: causing stress and concern – 176 (29%), worry about the loss of their personal data – 164 (27%)

[13] Base figures: unable to grow in line with previous expectations – 155 (26%), took over six months to get back on track – 184 (31%)

[14] % are out of a small business manufacturing respondent base of 144, retail of 123, financial services of 111, national of 599

Small businesses are under even more pressure than big organisations to get cyber security right.

69% of consumers surveyed in the North West say they are concerned about whether small businesses are as safe as bigger businesses

1 in 10 small businesses in Scotland and the North East say they aren't prepared for a cyber breach but it's not a concern

THE CYBER MYTH

We're too small to be a target

According to KPMG's recent SME Supply Chain research, 15% of procurement professionals said that they believe SMEs don't consider themselves as a target for cyber breaches due to their size.

THE REALITY

Businesses of any size are at risk, big or small. **60%** of small businesses surveyed have experienced a breach of some kind and with a lack of in-house IT expertise to protect work devices small businesses can be left exposed. This 60% finding is in line with the HMG Information Security Breaches Survey 2015, which found that 74% of small businesses had experienced an information security breach, costing them up to £75,000 – £311,000.

Small businesses are experiencing even more pressure to ensure they are adequately protecting their sensitive data.

60% of consumers surveyed have concerns about using small businesses, doubting that they are as cyber secure as bigger organisations.

Reliability and trustworthiness are crucial considerations for consumers choosing to buy from a small business. Yet consumers don't feel like small businesses are a safe pair of hands when it comes to their personal information; just 9% of consumers surveyed feel that small businesses are completely prepared for a cyber issue[15].

So what does this mean for small businesses?

They need to make cyber security a priority to reassure their customers that their data is secure. It is now part of their competitive offering and will only become more important in the future.

The regional snapshot

Compared to other regions, small businesses surveyed who were based in **Scotland** and the **North East** (10%) said they aren't prepared for a cyber breach but don't feel that this is a concern to them[16]. **Scottish** small businesses are the least likely to have taken steps to protect their data, with 19% surveyed admitting they haven't taken action, compared to the national average of 11% and just 4% in the **North West**[17].

Consumers surveyed based in the North West are more concerned than other regions about whether small businesses are as safe as bigger businesses (69% compared to the national average of 60%).

Consumers surveyed based in **Wales** and the **North West** value secure management of their information when buying from small businesses more than other regions (38% vs the national average of 34%)[18].

The sector snapshot

Compared to other sectors, the **design and creative** industries surveyed deem themselves the least at risk – 59% think it's unlikely that they'll be a target even though almost half (48%) have experienced a breach, versus 51% and 60% nationally. **Manufacturing** small businesses surveyed feel the most vulnerable – 59% think it's likely or very likely that they'll be a target for a cyber attack[19].

Those in the **retail** industry seem to be hit the hardest amongst those surveyed, taking the longest to resolve the issues the breach has caused at 33 hours, followed by life sciences at 26 hours. Two in five (42%) retail small businesses also said that it took more than six months for the business to recover, compared to 31% nationally[20].

[15] Base figures: consumers surveyed felt small businesses were 'completely prepared' for a cyber breach – 91 (9%); whereas 188 (19%) felt that large businesses are 'completely prepared' for a cyber breach.

[16] % are out of a small business respondent base by region of 100

[17] Base figures: small businesses in Scotland – 18 (19%), national average – 108 (11%), North West – 4 (4%)

[18] % are out of a consumer respondent base by region of 100

[19] % out of a small business respondent base by sector of 200

[20] Base figures: retail small businesses who took more than 6 months to recover – 52 (42%) out of 123

59% of small creative and design businesses surveyed think it's unlikely they'll be a target for a cyber breach

Small businesses in life sciences that experienced a breach say it took **26** hours to resolve

Many small businesses don't realise the wealth of sensitive data they have which puts them at significant risk of a cyber attack.

THE CYBER MYTH

We have nothing to steal

More than a **fifth of small businesses** (22%) surveyed don't consider data they hold to be commercially sensitive. This vastly underestimates the value of their information.

The information which the small businesses surveyed revealed they store on their systems which they do not consider to be commercially sensitive includes[21]:

- Intellectual property (29%)
- Supplier information (25%)
- Employee details (24%)
- Customer details (22%)
- Accounts information (22%)

THE REALITY

The vast majority (**95%**) of small businesses surveyed hold data in their IT systems. All of this is commercially sensitive and needs adequate protection against cyber crime threats.

Intellectual property data is held by almost half (45%) of the small businesses surveyed – from new products or services in the pipeline to new business ideas.

This is content that could fall into the wrong hands if not protected. Despite market competition and reputation being a key concern for small business owners, just **one in five (19%) say they would be immediately concerned about competitors gaining advantage** if they were breached.[22]

So what does this mean for small businesses?

If small companies aren't aware of the value of their data, and therefore not adequately protecting it, they are open to losing it all – and the consequences of this could destroy a small business. Customers lose trust, competitors get hold of information to gain advantage and hackers have access to all the company's financial details. Small businesses must safeguard the future of their firm by safeguarding their data.

29%
of small businesses in the North East say they don't consider their customer details to be commercially sensitive

The regional snapshot

Compared to other regions, more than one in four (29%) small companies surveyed who are based in the **North East** don't consider their customer details to be commercially sensitive, compared to the national average of 22%.[23]

The sector snapshot

A **quarter of the small financial services** businesses surveyed don't consider their accounts to contain commercially sensitive information – just under the national average of 22%. **Retail** small businesses surveyed are the least likely to consider both customer and IP details to be commercially sensitive (24% and 34% respectively say they don't consider it sensitive). Creative small companies place the most value on this data - just 21% and 22% respectively don't consider it to be commercially sensitive.[24]

25%
of small businesses surveyed in financial services say they don't consider their accounts to contain commercially sensitive information

22%
of small creative businesses say they don't consider their IP to be commercially sensitive

[21] Base figures: intellectual property – 293 (29%), supplier information – 253 (25%), employee details – 245 (24%), customer details – 224 (22%), accounts information – 216 (22%) do not consider this data to contain commercially 'sensitive' information

[22] Base figures: 75 (19%) of small businesses that have not experienced a breach (401)

[23] % are out of a small business respondent base by region of 100

[24] % are out of a small business respondent base by sector of 200

Protecting your business, your customers and your reputation.

So what does this information mean to small businesses?

Your business is sitting on a wealth of data that hackers can steal and sell on for a profit – from email addresses to financial records. Losing this data can have a huge impact on your company both in the short and long term. Not only could your data be sold to your competitors but having your data breached can affect your ability to attract new clients, new employees and even investment for the future.

Don't put your business and its reputation at risk by not protecting your data – follow these three simple steps and keep yourself secure:

- **Use three random words to create a strong password**
- **Install security software on all devices**
- **Always download the latest software updates**

Companies can also take advantage of **free online training courses** for staff, **Cyber Essentials** and a **simple cyber security guide** for small and medium-sized firms. Cyber Essentials is a Government-backed and industry supported scheme designed to help businesses protect themselves against the most common cyber threats. Gaining accreditation enables businesses to display the Cyber Essentials badge and demonstrate to their customers they take their cyber security seriously.

For more information on keeping your business secure visit:

www.cyberstreetwise.com
www.kpmg.com/uk/cyber
www.cyberstreetwise.com/cyberessentials

Research methodology

The consumer and small business research was commissioned by Cyber Streetwise and KPMG in December 2015. The small businesses and consumers were all based in ten key regions of the UK: Wales, Scotland, London, South East, South West, East Anglia, West Midlands, North East, North West and Yorkshire and Humberside.

The small businesses surveyed were:

- Senior decision makers in businesses with up to 25 employees (including sole traders)
- Operating in the manufacturing, financial services, life sciences, retail and design/ creative sectors

This was an online survey carried out by a third party research agency. 1,000 small business and 1,000 consumers completed the survey, with their responses then determining which questions they subsequently answered. The findings in this report refer only to the small businesses and consumers surveyed which should be considered when applying the findings to the wider business and consumer sectors.

Supply Chain research conducted amongst procurement leaders in organisations with 250+ staff was delivered by KPMG and 3Gem in September 2015.

I found out that around 80% of cyber breaches could be stopped by adopting some of the basics so we made a few changes to boost our cyber security. Data is the lifeblood of our business and we simply couldn't afford the reputational damage if something were to happen to it.

Duncan Sutcliffe, Sutcliffe & Co Insurance