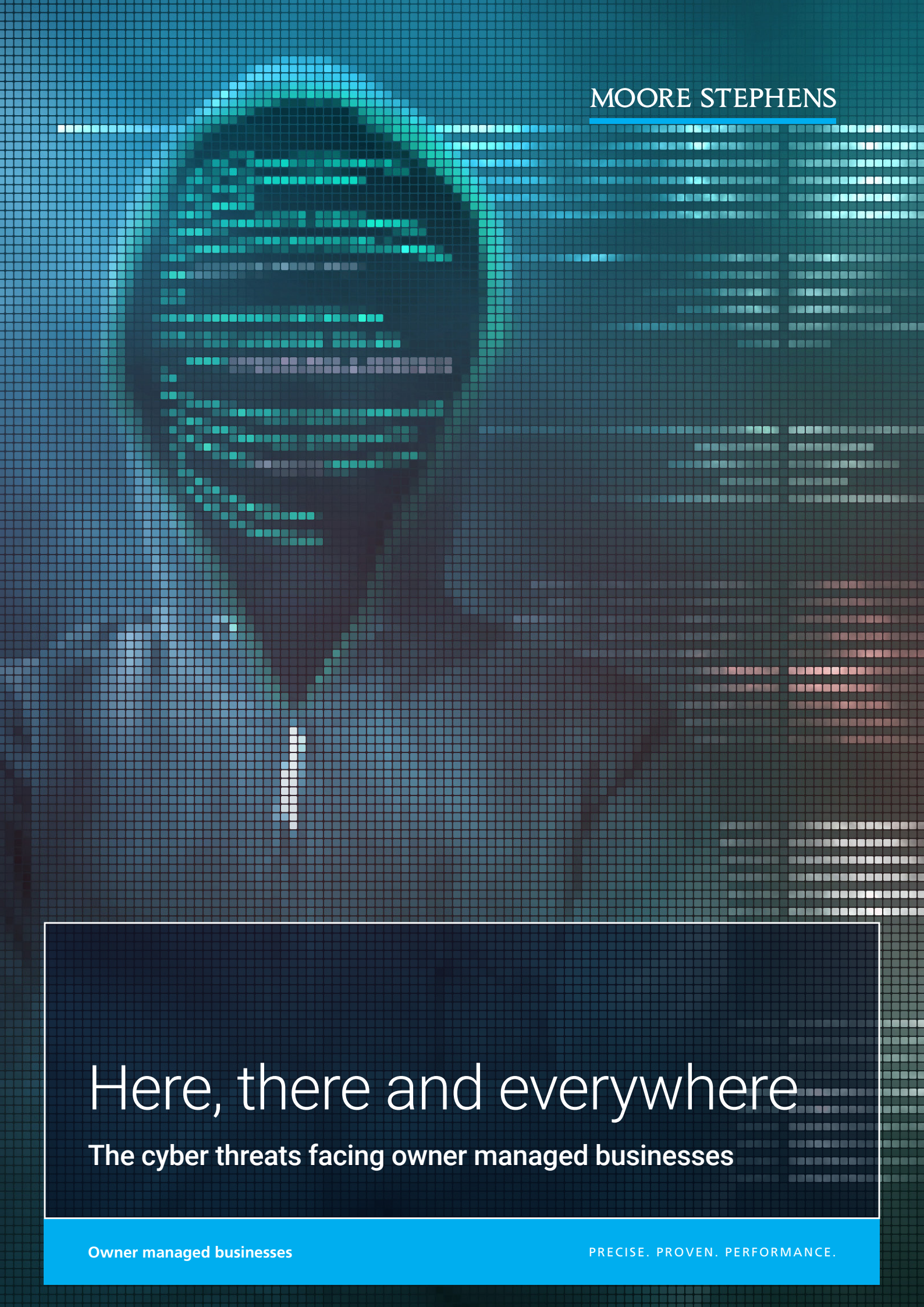


MOORE STEPHENS

Here, there and everywhere

The cyber threats facing owner managed businesses

Owner managed businesses

PRECISE. PROVEN. PERFORMANCE.

Table of contents

Survey details

We conducted an online survey of OMBs across a wide range of industry sectors between 18 July and 11 August 2017, receiving 115 responses. Participants include CEOs and managing directors, founders, owners, partners and other directors, managers and chairmen.

Foreword

Mark Lamb
Head of Owner Managed Businesses
M: +44 (0)7967 727 501
E: mark.lamb@moorestephens.com

When cyber-attacks and data breaches hit the news, they invariably involve the largest businesses or national institutions like the NHS. But this doesn't mean owner managed businesses are not under threat too. Every OMB, regardless of size or industry sector, is at risk.

At Moore Stephens, we work so closely with OMBs, and want to make sure they are fully aware of the threats they face every day, in the ordinary course of business. You do not need to be doing anything particularly sophisticated to be at risk. Simply clicking a link in an email can leave you vulnerable to a data security breach.

Part of the challenge for OMBs (as for all businesses) lies in the fact that hackers and cyber criminals do not just target specific companies with their attacks. Many forms of malware (malicious software) can trawl the internet looking for vulnerable websites and computers. No one needs to have a specific grudge against you. That said, a 'malicious insider' – a member of staff disgruntled for some reason – is also a risk that can never be fully ruled out.

In this report, we wanted to see how aware OMBs are about the risks they face, how they have responded to problems and what they fear most. We have found that while OMBs are exposed to the risk of cyber-attack and data loss in many ways, most are highly aware of the threats around them. This is encouraging. However, more worrying is the fact that 31% do not know what action to take to protect themselves from the threats they see.

What is really important now is that all OMBs take the basic and essential steps to establish and maintain their cyber-attack and data loss defences – setting policies, maintaining controls and training staff. No defences can be 100% secure, but they can go a long way towards preventing breaches and the unnecessary costs, business disruption and damaged reputations that follow.

Now is the time for OMBs to take action, review all areas that could be at risk and prepare robust defences. After all, over 40% of OMBs like you have already been victims.

Executive summary

Awareness of cyber and data risks has been heightened by recent high profile cases, with OMBs recognising the rising threat to their businesses.

- Just 33% agreed and 67% of OMBs disagreed with the statement "When I hear about a big company suffering a cyber-attack or data breach – it doesn't feel relevant to my business", with 82% disagreeing with the statement "We are too small to be targeted".
- OMBs report that malicious code (83%), computer viruses (82%) and phishing email scams (80%) are the key threats that they are aware of and that pose the biggest threat to their business.
- 30% of OMBs surveyed have already suffered from a targeted or malicious cyber-attack and 21% have experienced an inadvertent data loss or error. Overall, 41% have suffered one or both of these problems.
- In the event of a cyber-attack or data breach, OMBs are most worried about loss or damage to accounting data, files or client databases (77%), disruption to business plans (69%) and disruption to client relationships (64%).
- Of those that have suffered a cyber- attack or data breach, just 26% reported it to the police, with just 23% reporting the incident to their insurer, indicating that OMBs have concerns relating to the impact on reputation and client relationships.
- Those that have suffered an attack or breach are investing in additional prevention software (79%) and staff training (70%), recognising that an emphasis on protection and prevention is just as important as recovery.
- The majority (57%) of OMBs recognise that they do not need to be specifically targeted to be a victim, and that simple human error is a real threat.
- 68% of small OMB business leaders recognise their current cyber prevention isn't sufficient – and that they'd benefit from cyber insurance to help their business recover. But only 26% have already invested in it.

OMBs are at risk

Owner managed businesses are exposed to the risks of cyber-attack or data loss in many ways.

> *You should always ask about the security measures being applied by your outsourced service provider. It's a matter of basic due diligence.*
>
> **Steve Williams**
> Partner, Moore Stephens London

75% of OMBs regularly make BACS payments to suppliers. What they may not know is that if any fraud occurs in relation to these payments – say the money doesn't go where it should have – the OMB carries the cost. Unlike with credit card payments, banks make no guarantees around recovery.

"Our research finds that 70% of OMBs use email to send business-critical information," says Steve Williams, a partner at Moore Stephens London and an IT risk expert. "Email is unencrypted, so using it to send business-critical information creates an automatic vulnerability."

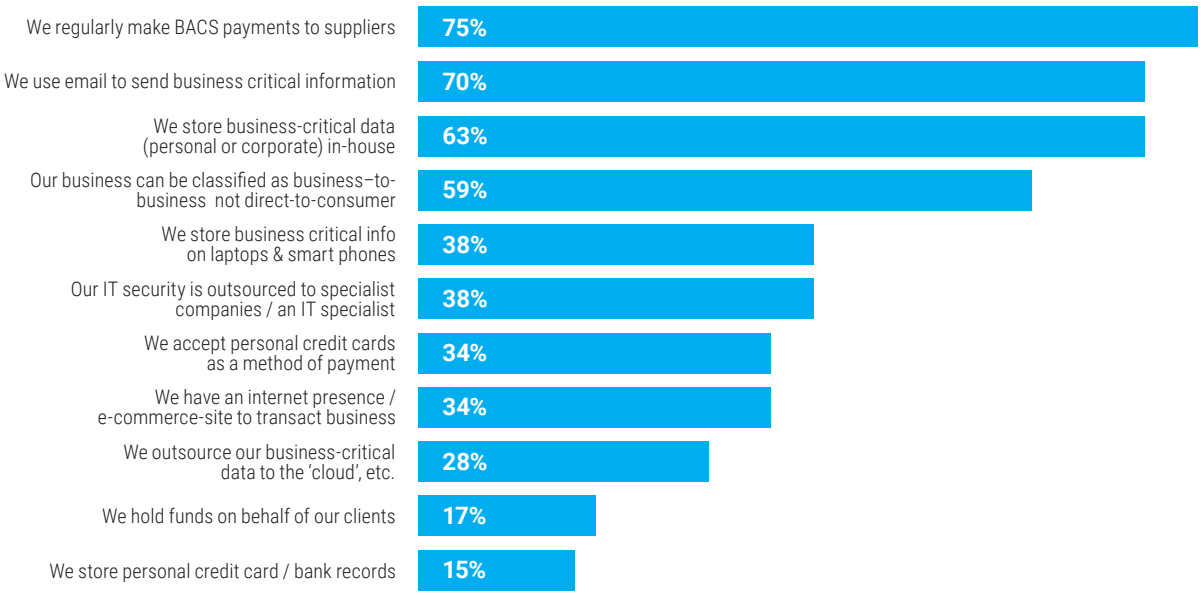
These aren't the only vulnerabilities that OMBs have: 38% of OMBs store business critical information on laptops and smart phones. Given how easily devices can be lost or stolen, these OMBs are at risk of losing potentially private data.

Of the OMBs we surveyed, 63% store business-critical data (personal or corporate) in-house, so need to make sure they are protecting it properly by keeping their IT security up to date. The 28% of OMBs that outsource their business-critical data (e.g. to the 'cloud') aren't off the hook, however. Their IT security problem doesn't necessarily transfer to the outsource service provider. Under tougher data protection regulations that become effective in 2018, the EU General Data Protection Regulation (GDPR), businesses will have a new legal obligation to know that their service provider is competent and capable of handling their data properly.

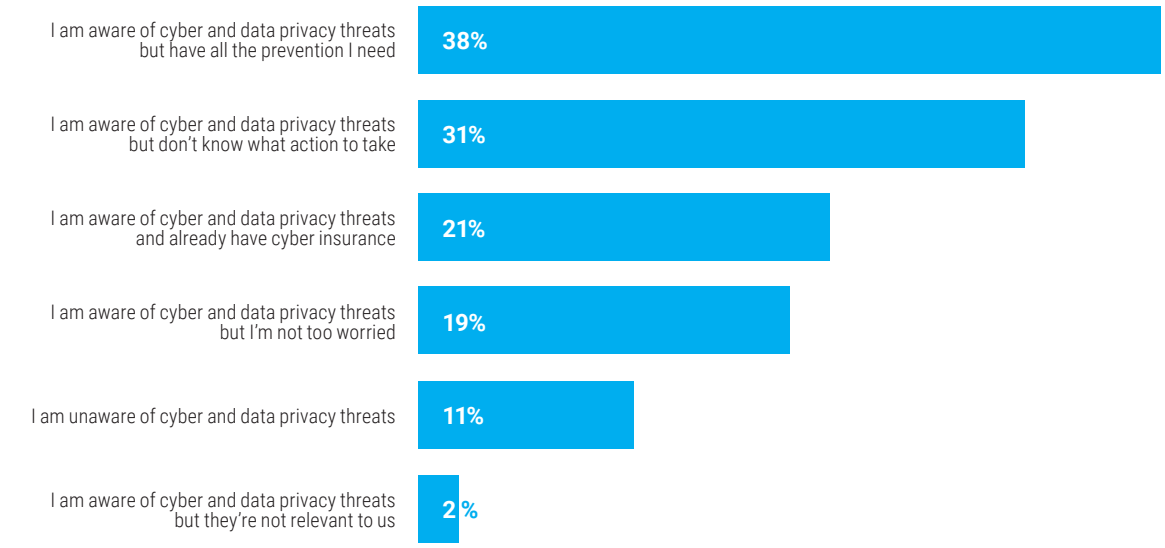
OMBs are at risk

Owner managed businesses are exposed to the risks of cyber-attack or data loss in many ways.

Which of the following best describes your business currently?



Which of the following statements apply to your business?



Cyber threats come in many forms

Just 11% of OMBs say they are unaware of the cyber and data privacy threats facing their business.

Our survey aimed to establish how aware OMBs are of specific cyber risks and, if so, which they see as being threats to their business. We found awareness levels to be high, particularly with regards to:

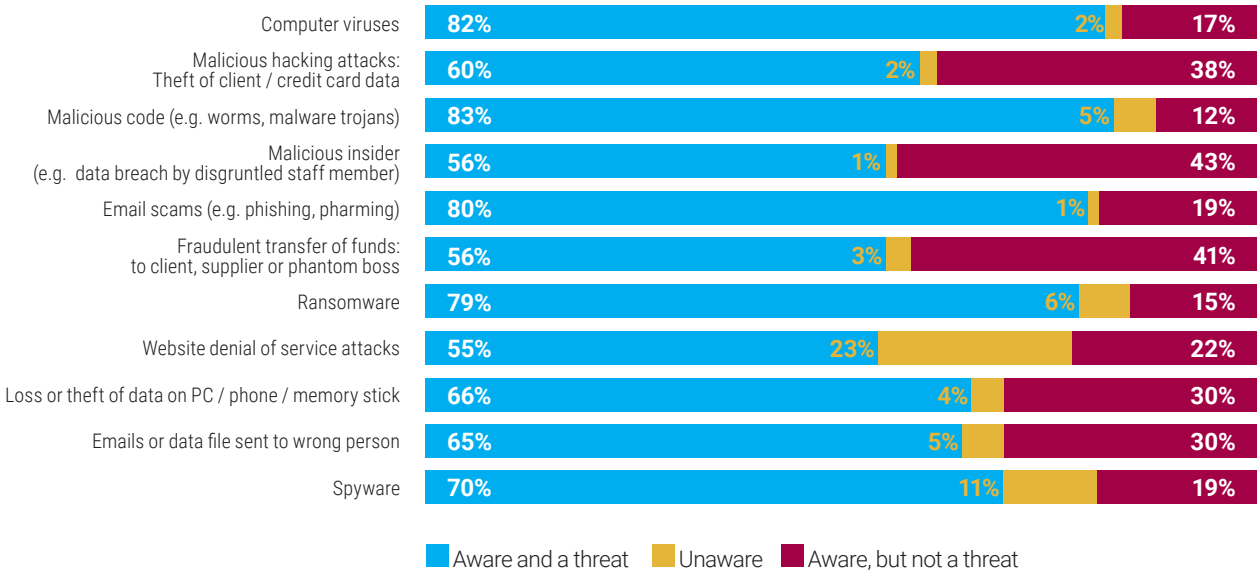
- malicious code, such as worms or malware trojans (83%);
- computer viruses (82%);
- email scams (80%);
- ransomware (79%).

The headline news about the ransomware attacks suffered by the NHS in May 2017 seem to have made an impression on OMBs.

Even so, OMBs may be under-estimating some of the threats facing their business closer to home, particularly the threat posed by malicious insiders (e.g. a data breach by a disgruntled member of staff). 43% of OMBs say they are aware of the risk of malicious insiders, but say it's not a threat. Similarly, 41% of OMBs feel they are aware fraudulent transfers of funds to clients, suppliers or phantom bosses, but do not believe it's a threat.

It's noticable that OMBs that have already suffered a targeted or malicious cyber-attack (or an inadvertent data loss) are more likely to be aware and see the threat from other, future forms of attack.

Which of the following cyber risks have you heard of / do you feel might be a threat to your business?



The threat is real

So how many OMBs have suffered at the hands of cyber criminals?

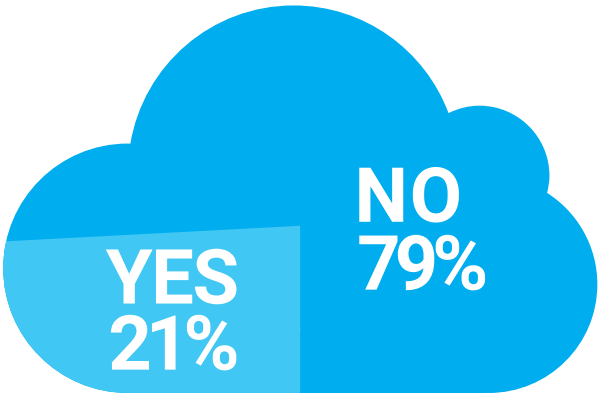
It's encouraging that only 18% of OMBs think they are too small to be targeted and that only 15% don't think they have anything a cyber-criminal would want to steal. Random attacks don't discriminate by size and anyone could be hit.

Steve Williams
Partner, Moore Stephens London

Among the OMBs we surveyed, 30% have already suffered from a targeted or malicious cyber-attack and 21% have experienced an inadvertent data loss or error. Overall, 41% have suffered one or both of these problems. These results are in line with the Government's Cyber Security Breaches Survey 2017, which found that 46% of all UK businesses identified at least one cyber security breach or attack in the last 12 months.

Has your current business ever suffered from a cyber or data privacy issue?

A targeted / malicious cyber attack



An inadvertent data loss / error

No business is too small

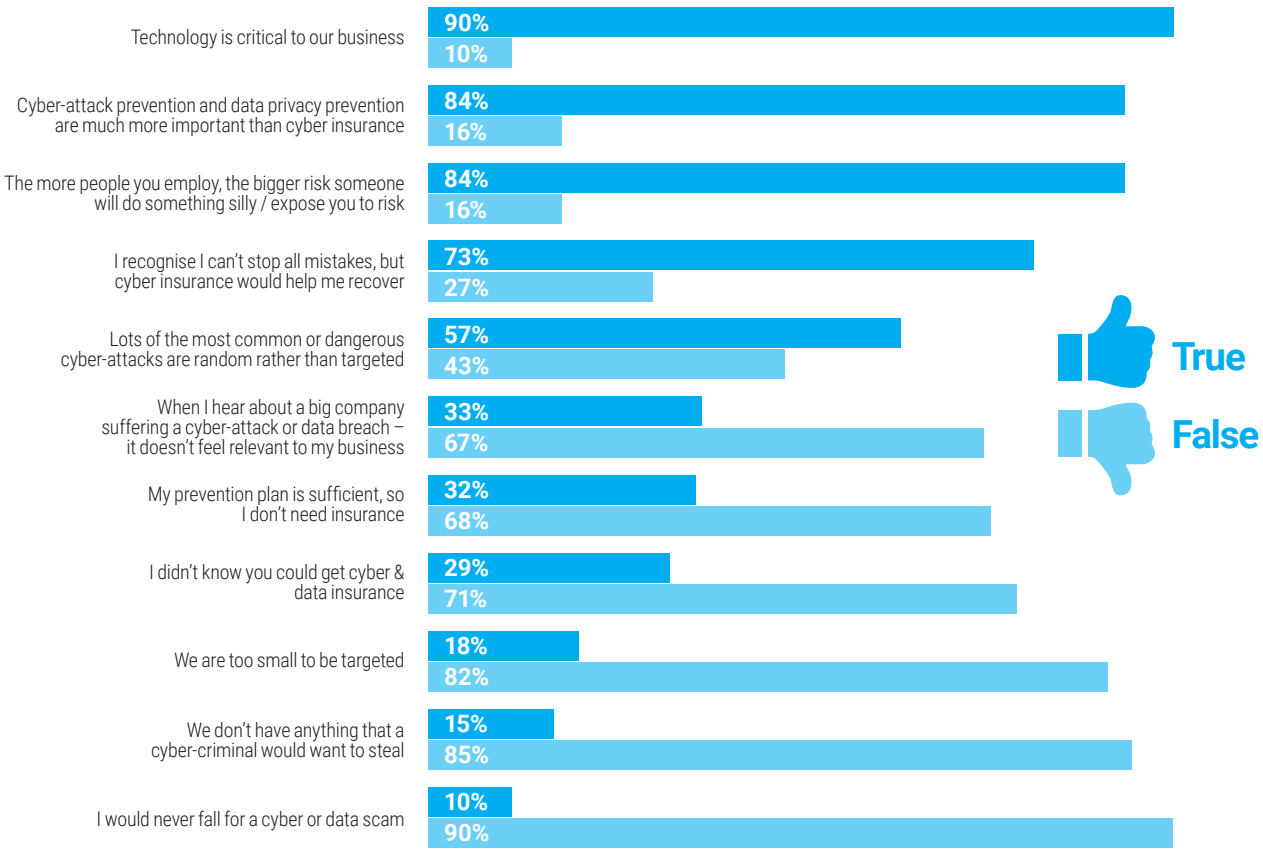
Although some OMBs may not appreciate their real exposure to all threats, many have 'wised up' to the general cyber risk.

Over half (57%) recognise that the most common or dangerous cyber-attacks are random rather than targeted. Hackers and criminals can trawl the internet looking for entities that have failed to maintain their cyber defences: failing to download a 'patch' can leave OMBs exposed.

"It's also encouraging that only 18% think they are too small to be targeted and that only 15% don't think they have anything a cyber-criminal would want to steal," Steve Williams, partner at Moore Stephens London comments. "Random attacks don't discriminate by size and anyone could be hit."

Only 10% of OMBs surveyed think they would never fall for a cyber or data scam – but they need to think again. "We all could," Williams says. "Even cyber risk experts."

Which of the following statements best describe your views?



Cyber and data breaches have real business impacts

Cyber-attacks and data breaches can clearly have a big impact on businesses. They can disrupt business plans and damage business reputations. OMBs are right to be concerned about costs too. Once you've suffered a breach, you realise how much it costs to address it.

Steve Williams
Partner, Moore Stephens London

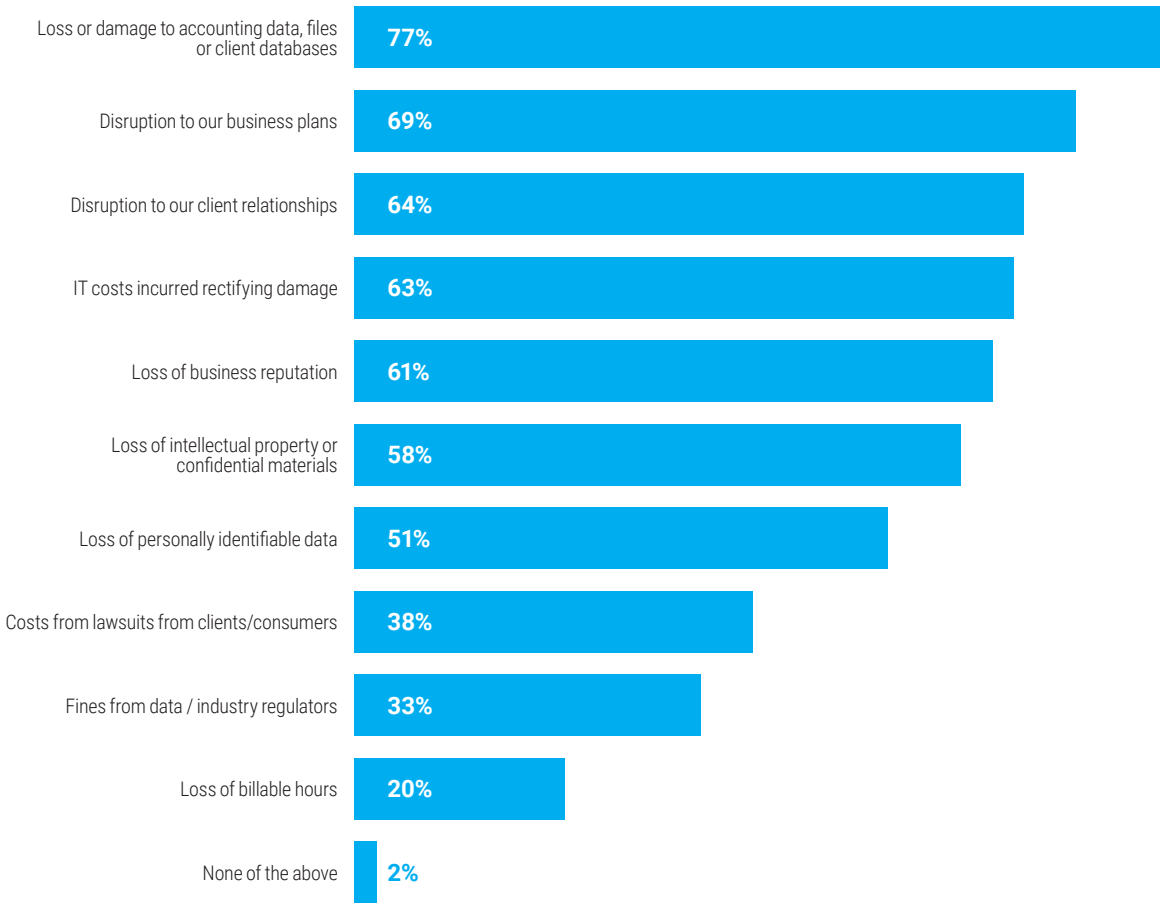
We asked OMBs what they would be most worried about if they were to suffer a cyber-attack or data privacy breach. Loss or damage to accounting data, files or client databases is the top concern (77%), followed by disruption to business plans (69%), disruption to client relationships (64%), IT costs incurred rectifying damage (63%) and loss of business reputation (61%).

OMBs that have already suffered a cyber-attack or data loss are more likely to be worried about all these issues, but particularly more worried about IT costs incurred rectifying damage (72%) and the loss of business reputation (72%).

These OMBs are right to be concerned. According to recent Government research, the average business faces costs of £1,570 as a result of cyber security breaches – ranging from £19,600 for the average large firm to £1,380 for the average micro and small firm.

Cyber and data problems have real business impacts

In the event of cyber-attack or data privacy breach, which of the following would most worry you?



How are OMBs responding?

Investing in staff training and increasing awareness are the keys to a robust defence.

It's good news that OMBs are investing in training their staff, because staff awareness and behaviours are the key to a strong defence.

Ashley Conway
Partner, Moore Stephens Stoke

OMBs that have suffered a targeted or malicious cyber-attack or an inadvertent data loss or error responded in a number of ways, but primarily by investing in additional prevention software (79%) and staff training (70%).

It is a concern, however, that only 26% of OMBs reported their incident to the police. "This means that some OMBs suffered a malicious or targeted attack, but didn't report it," Steve Williams, partner at Moore Stephens London says. "People should tell the police. It's a crime, just like a burglary, so reporting it is a good way to access help and support." The easiest way to report an incident is through the website of ActionFraud, the UK's national fraud and cybercrime reporting centre (see www.actionfraud.police.uk).

Of the OMBs that suffered a cyber-attack or data loss incident, just 9% invested in the services of post cyber-attack recovery specialists. In matters of cyber-attacks and data loss, using specialists is always recommended. The low usage rate suggests many OMBs don't know these services are available or don't know how to find them. While existing insurance policies such as commercial property, business interruption or professional indemnity insurance, may provide some elements of cover against cyber risks, businesses are increasingly buying specialised cyber insurance policies to supplement their existing insurance arrangements, particularly if they:

- hold or process sensitive details of customers or employees, such as national insurance numbers, banking or medical information;
- rely heavily on IT systems and websites to conduct their business;
- process payment card information.

ONLY 26% OF OMBs REPORTED A CYBER OR DATA BREACH TO THE POLICE

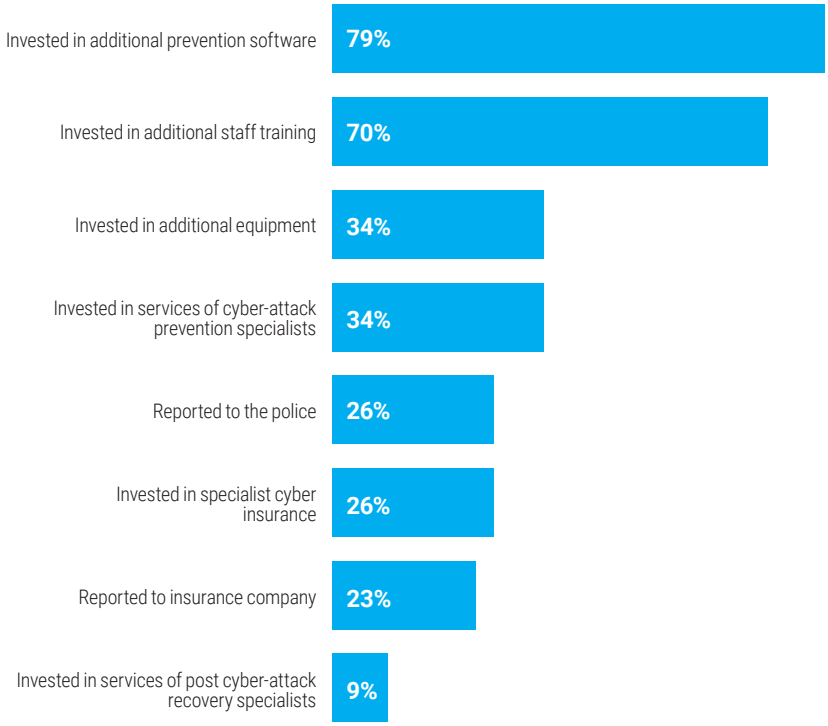
How are OMBs responding?

Understanding your options once you've suffered an attack or breach can help your business get back on its feet.

Matthew Norris, insurance underwriter for small businesses at specialist insurer, Beazley explains: "There are basically two types of cyber insurance available. One concentrates on making payments in the event of an attack or breach, whilst the other provides what OMBs really need in the aftermath of a cyber-incident – urgent access to a specialist team who can respond to the incident.

"Cyber incidents are incredibly varied, and the threats can change quickly. We believe the greater experience you have access to, the smaller the financial and reputational consequences for your business."

After you suffered an attack, what additional actions did you take as a result?



An insurer's view

Matt Norris
Underwriter, Beazley
E: matthew.norris@beazley.com

Moore Stephens' research re-enforces our view that owner managed businesses are becoming increasingly aware that data breaches, and other cyber incidents, can happen in a variety of ways to both small and large companies, often through human error, and without malice.

As well as investing in prevention tools, OMBs need to have a plan about how to keep their business up and running, should something go wrong. What's worrying is that 73% of owner managed business leaders recognise they cannot stop all mistakes, and almost two thirds of OMBs recognise that their current prevention plans are not sufficient.

So the question is, do you have the time money and resource to manage the response when the inevitable happens? Or would you benefit from access to a team who can help manage the problem, and let you focus on your business?

This report finds that just 9% of OMBs that suffered an attack invested in the services of post cyber-attack recovery specialists, so what steps should the remaining 91% be taking to protect their business?

Most regulators understand that even the best run companies can suffer from a cyber-attack or breach, but rarely forgive an ineffective response – which could in turn lead to a regulatory investigation, leading to further disruption to your business. Under the EU GDPR regulation due to be in force in May 2018, it states that notice of a data breach must be provided 'without undue delay and, where feasible, not later than 72 hours after having become aware of it.' If notification is not made within 72 hours, the data controller must provide a 'reasoned justification' for the delay.

Typically when businesses suffer a cyber-attack or data breach, there are two stages that then occur from an insurance perspective:

1. First costs are incurred investigating and reporting;
2. Legal suits may be filed, or complaints made.

We have found that the first stage is an opportunity to limit the adverse consequences of the second stage, a stage that could be expensive and disruptive to a company. An effective response team should maximise that opportunity to limit the adverse consequences.

An experienced response team should allow a quick but sophisticated response, which we believe is essential to minimise disruption to your business, satisfy regulators and manage your business' reputation.

Are you protected?

Paul Latarche
Head of Insurance, Moore Stephens
E: paul.latarche@moorestephens.com

Most businesses assume that they are covered against cyber-related incidents through their general insurance policy, but in many circumstances, this is not the case - as losses caused by a hacking attack will not be included.

Given the gaps in standard cover and the extent of the cyber threat to all businesses, it's no surprise that cyber insurance is one of the fastest growing lines of cover in the market. As our research shows, OMBs are increasingly recognising the threats they face and the insurance market is responding.

However, taking out cyber insurance isn't quite as simple as obtaining household or car insurance, due to the range of options of cyber cover available. Not all cyber policies, for example, will compensate you for business interruption (perhaps caused by a ransomware attack), so determining what type of cover is right for your business is vital.

If your business trades online, takes credit card payments or holds customer data, your exposure is likely to be significantly increased. If the customer details you hold are hacked, your client's response may well be to take their custom elsewhere – and if all your customers follow suit, then your business could be wiped out. To protect yourself against this doomsday scenario – taking out an insurance policy that covers the additional costs of PR and other essential clear-up actions could prove extremely valuable to the survival of your business.

As our research indicates, OMBs understand that every business – large or small - is likely to be at risk from a cyber-attack or data breach. Fraudulent emails purporting to be from a supplier, a colleague, the accounts department or even the boss are widespread, and haven been proved to trick people into authorising false payments.

Prevention is always the best solution, of course, so it's vital to establish policies and procedures to mitigate your risk as far as you can. Make sure your staff are properly trained so that they are more likely to spot attempted frauds and cyber-attacks and can avoid the traps being set for them. But if those traps succeed, cyber cover then provides a welcome safety net.

Conclusion: OMBs must protect themselves

Spend some time deciding what type of cyber incident would be of greatest concern to your company. After you have decided, you can choose to accept that risk, to reduce the likelihood by investing in prevention or to transfer the risk to a third party to manage.

Matt Norris
Underwriter, Beazley

Around one in five (19%) of the OMBs we surveyed say they are aware of cyber and data privacy threats but are "not too worried". Given the nature of the threat, they should be. Establishing sound controls, training staff and keeping up with software updates are all vital bricks in the defensive wall, but even the best protected OMBs can't guarantee their IT security. Fraudsters and hackers keep on innovating, so today's defences could well be inadequate tomorrow, while human error can never be ruled out.

Realising their exposure, 21% of OMBs have taken out cyber insurance (36% of those that have experienced a malicious cyber-attack or inadvertent data loss). Although prevention is always better than cure, taking out insurance in advance of a cyber-attack or data loss could help OMBs to recover more quickly and effectively.

It's a huge concern that 31% of OMBs in this survey are aware of cyber and data privacy threats but say they don't know what action to take. Advice is widely available and even free. A useful source of help is the government-endorsed Cyber Essentials scheme (see www.cyberaware.gov.uk/cyberessentials). If professional expertise is needed, then it's best to look for specialists in cyber-attacks and data loss (whether to help with prevention or recovery), rather than assuming general IT service providers have the necessary expertise.

The threat of cyber-attacks and the risk of data loss are real for OMBs. Taking action to address the many threats and risks should be a high priority for all.

Our solutions for OMBs

Our in-depth understanding of the challenges facing OMBs allows us to deliver focused accounting and advisory solutions, both locally and globally.

51% of OMBs are worried about the loss of personally identifiable data

Under tougher data protection regulations that become effective in 2018, the EU General Data Protection Regulation (GDPR) will bring with it new legal obligations and large fines.

Our GDPR health check will help you establish where the risks lie, what actions are to be taken and how to achieve compliance before May 2018.

30% of OMBs have already suffered from a target or malicious cyber-attack

OMBs that have suffered a cyber-attack will know that half the battle is knowing where to turn for help; a decision that is critical in reducing the negative impact on your business.

We offer an incident response service to help with just that, and provide a team on standby to help you get back on your feet and discover exactly what went wrong.

79% of OMBs invested in additional prevention software to stop cyber attacks

Prevention software can be expensive and in many cases fails to address the real issues within your IT systems. By mirroring the actions of a would-be hacker, we can probe your systems and find the vulnerabilities that are at risk of being exploited, leaving you with a detailed report listing the priority areas of your systems that need to be addressed.

70% of OMBs invested in training following a cyber-attack

Staff awareness is the key to a robust cyber defence, but the challenge lies in training your staff in advance against an attack. We apply our real world experience to cyber training, having dealt with many different types of attacks and breaches. We will train and advise your staff on how to be cyber savvy.

31% of OMBs are aware of cyber and data privacy threats but say they don't know what action to take

We know that many OMBs simply don't have the resources to effectively manage their own cyber security. Our team, with years of experience, can alleviate that burden and run your security for you, leaving you to focus on strengthening and growing your business.

77% of OMBs are worried about loss or damage to accounting data, files or client databases following a cyber-attack

Understanding your environment and your resilience to cyber-attacks is a key first step in identifying the gaps in your processes and technology.

Our Cyber health check is designed to help you identify the risks facing your business, and will provide practical, actionable advice on how to address them.

Ten top tips to protect your business

1. **Run software updates and apply patches**
   Software updates are vital. Software vendors address vulnerabilities fast, so if you update your software straight away, you're likely to frustrate attackers.

2. **Update anti-virus protection**
   Anti-virus protection installed on your computer is a fundamental starting-block for good cyber security. Anti-virus companies are quick to update their systems to catch the latest viruses, so make sure you keep updating.

3. **Filter content**
   Filter the content your employees can access – by blocking potentially harmful sites and files – to protect yourself from unknown threats.

4. **Make the most of password managers**
   Use a password manager to create different and strong passwords for each website you visit – so if one account is compromised, the others remain safe. Two factor authentication reduces the likelihood of getting hacked even further.

5. **Protect your banking payments**
   Some banks can reject suspicious payments if account numbers are changed, but the account name stays the same. The default setting for this protective function may be 'off', so turn it on if you want to benefit.

6. **Use encryption**
   As a general rule, if a message leaves your office it needs to be encrypted. Most modern computers and mobile phones include encryption, so make sure it's switched on.

7. **Get ready for new data regulations**
   Make sure you know your GDPR responsibilities – or risk a maximum fine of 20 million euros or 4% of annual turnover (whichever is greater).

8. **Check your supply chain**
   Check that members of your supply chain have the right certifications to look after your information. Cyber Essentials (www.cyberaware.gov.uk/cyberessentials/) is a good starting point.

9. **Think before you click**
   Everything can be undone by human error. The best way to protect yourself is to think before you click – particularly before sending emails.

10. **Focus on the basics**
    Don't worry about getting the latest 'must have' cyber product. Your organisation will able to fend off most cyber-attacks if you do the basics well.

About Moore Stephens

We help you thrive in a changing world.

Our objective is simple: to provide all the support and guidance needed to deal with new risks and opportunities. We ensure easy access to the right people, so decisions can be made quickly and confidently. A consistent team will partner with you to support your aspirations and contribute to your success.

You'll have access to a range of core services, including audit, accounting, tax, risk and systems assurance, corporate finance, restructuring and insolvency, wealth management and disputes analysis. We support a broad range of individuals and entrepreneurs, large organisations and complex international businesses.

If your business and personal interactions need to expand, we'll help make it happen – coordinating advice from a network of offices throughout the UK and in more than 100 countries.

Moore Stephens globally
You'll have access to the resources and capabilities to meet your global needs. By combining local expertise and experience with the breadth of our UK and worldwide networks, you can be confident that, whatever your requirement, we provide the right solution to your local, national and international needs.

About Beazley
Beazley has been at the forefront of specialist insurance for over three decades and is a market leader in many of its chosen lines such as cyber. In 2016 Beazley underwrote gross premiums worldwide of $2,195.6 million and has operations in Europe, the US, Canada, Latin America, Asia and Australia.

MOORE STEPHENS

www.moorestephens.co.uk