HM Government

Ipsos MORI
Social Research Institute

University of Portsmouth

May 2016

Cyber Security Breaches Survey 2016

Main report

Dr Rebecca Klahr, Sophie Amili and Jayesh Navin Shah
Ipsos MORI Social Research Institute

Professor Mark Button and Dr Victoria Wang
Institute for Criminal Justice Studies, University of Portsmouth

The Cyber Security Breaches Survey 2016 has been endorsed by the following organisations.

Across the UK, the Confederation of British Industry (CBI) speaks on behalf of 190,000 businesses of all sizes and sectors. The CBI's corporate members together employ nearly 7 million people, about one third of private sector-employees. With offices in the UK as well as representation in Brussels, Washington, Beijing and Delhi, the CBI communicates the British business voice around the world.

The Federation of Small Businesses (FSB) is the UK's leading business organisation. It exists to protect and promote the interests of the self-employed and all those who run their own business. FSB is non-party political and is also the largest organisation representing small and medium sized businesses in the UK. Small and medium-sized businesses make up 99.9 per cent of all businesses in the UK, and make a huge contribution to the UK economy. They account for 47 per cent of private sector turnover and employ 60 per cent of the private sector workforce.

ICAEW is a world-leading professional membership organisation that promotes, develops and supports over 145,000 chartered accountants worldwide. ICAEW's IT Faculty represents chartered accountants' IT-related interests and expertise, contributes to IT-related public affairs and helps those in business to keep up to date with IT issues and developments, including cyber security. For more information about ICAEW's work on cyber security, please visit icaew.com/cyber.

Foreword

Ed Vaizey MP

Welcome to this new Cyber Security Breaches Survey.

The UK's digital economy is strong and growing, with more and more firms embracing the internet to do business and find new customers. Businesses are improving productivity and getting more efficient by using digital technologies. UK consumers are the biggest internet shoppers in Europe, with four in five people buying something online in the past year.

I am proud British industry is leading the way. But to secure our place in today's global marketplace we need to ensure the UK is one of the safest places in the world to do business online. Too many businesses are suffering disruption, financial loss and theft of intellectual property as a result of cyber crime. This is why the Government has announced a new £1.9 billion investment in cyber security over the next five years. This will help to make the UK the best protected country in cyber space.

We can only do this in partnership, which is why Government is working closely with industry, academia and law enforcement to tackle the problem. This survey is part of our joint effort to understand the cyber threat and identify the actions we need to take.

There is a lot of good news in this survey. Businesses recognise cyber security needs to be a high priority and nearly half have technical controls in the five areas set out in the Government's Cyber Essentials scheme. Clearly there is still much work to be done, so I want businesses to change their behaviour as a result of this survey. When I speak to businesses it is clear awareness of the cyber threat is now very high. Everyone I talk to agrees the threat is significant and needs to be tackled, but there is a gap between awareness and action, which is highlighted in this report. We see a steady stream of breaches and attacks on firms which assume they are on top of security, but still haven't got a good understanding of the possible impact on their business or what they should do about it.

The Government has made it easier to get the basics in place. There is now a wide range of free guidance and training on the gov.uk website. Our Cyber Essentials scheme shows firms how to protect against common Internet threats and gives them a way to demonstrate to their customers and investors that they are taking the risk seriously. All businesses operating online, selling goods and services online, or storing customer details and personal data, should aim to adopt Cyber Essentials as a minimum. The Government already mandates this for many of its suppliers and I hope many more firms will encourage their suppliers to adopt the scheme too. By doing this we can significantly improve the cyber security of UK business.

This new survey represents our best current evidence on the state of industry cyber security and the need for businesses to take action. I hope it helps to inform industry, policymakers, cyber security specialists and everyone else who is working together to protect the UK online.

Ed Vaizey MP, Minister for the Digital Economy

Contents

List of Figures

List of Tables

Key findings

69% of businesses say cyber security is a high priority for senior managers

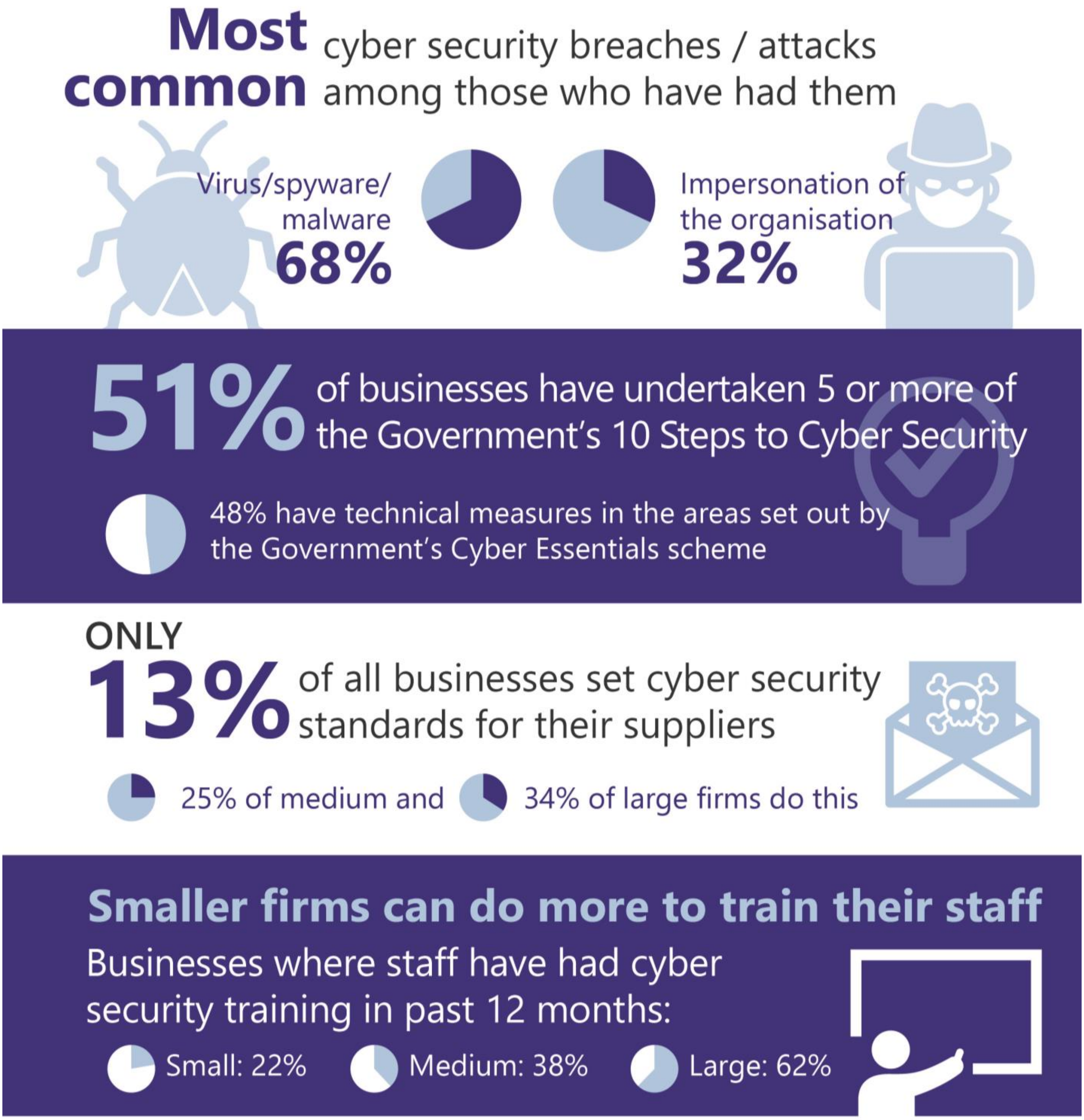
- But only 51% of companies have taken recommended actions to identify cyber risk
- Only 29% have formal written cyber security policies
- Only 10% have a formal incident management plan

65% of large firms detected a cyber security breach or attack in the past year

- 25% of these experience a breach at least once per month

£3m the most costly breach identified in the survey

- Average cost of a breach to large businesses = £36,500
- Only 5% of firms have ongoing monitoring of breach costs



Most common cyber security breaches / attacks among those who have had them

Virus/spyware/ malware **68%**

Impersonation of the organisation **32%**

51% of businesses have undertaken 5 or more of the Government's 10 Steps to Cyber Security

48% have technical measures in the areas set out by the Government's Cyber Essentials scheme

ONLY **13%** of all businesses set cyber security standards for their suppliers

25% of medium and 34% of large firms do this

Smaller firms can do more to train their staff

Businesses where staff have had cyber security training in past 12 months:

Small: 22% Medium: 38% Large: 62%

Graphics produced by HM Government

Summary

This report details the findings from quantitative and qualitative research with UK businesses on cyber security. The research was commissioned by the Department for Culture, Media and Sport, as part of the National Cyber Security Programme. It was carried out by Ipsos MORI, in partnership with the Institute for Criminal Justice Studies at the University of Portsmouth, and comprised:

- a representative telephone survey of 1,008 UK businesses from 30 November 2015 to 5 February 2016
- a total of 30 in-depth interviews undertaken in January and February 2016 to follow up businesses that participated in the survey.

A sizable majority of businesses recognise the importance of cyber security

E-commerce has become much more important to UK businesses in recent years. Office for National Statistics data shows that in 2014, e-commerce sales were £573 billion across non-micro businesses, versus £335 billion in 2008.[1] In this Cyber Security Breaches Survey, half (53%) of all businesses say online services are a core part of the goods and services they provide, at least to some extent.

In this context, seven in ten businesses (69%) say cyber security is either a very high (33%) or fairly high (37%) priority for their organisation's senior management. The qualitative findings highlight various factors that have helped businesses to understand the importance of the issue:

- media stories around high-profile breaches and their consequences
- key individuals in the organisation, particularly on company boards, helping to champion the issue
- recognising cyber security as a business performance issue or as good business practice, rather than solely as an IT problem
- a staff culture that emphasises customer confidentiality and good data management.

Many businesses have not yet taken appropriate actions around cyber security

While businesses by and large see cyber security as important, many may not fully understand how their organisation is at risk and what action to take. Just half (51%) of all businesses have attempted to identify the cyber security risks faced by their organisation, for example through health checks, risk assessments or audits. However, this is higher among medium firms (78%) and large firms (94%).[2]

Most businesses have some form of rules or controls in place around cyber security, although these can still fall short of best-practice standards:

[1] See http://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/ecommerceandictactivity/2014.

[2] Analysis by size splits the sample into micro businesses (2 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more).

- Half of all firms (48%) have enacted basic technical controls across all five areas laid out under the Government-backed Cyber Essentials scheme.[3] While it is commonplace for businesses to regularly update software (88%) and malware protections (83%), and to have configured firewalls (85%), it is less common to find businesses that restrict IT access to specific users (77%), or place security controls on company-owned devices (62%).

- Half (51%) have undertaken five or more of the steps in the Government's 10 Steps guidance, although just five per cent have made progress on all 10.[4] Many businesses can do more to formalise their approaches in line with the guidance – just three in ten (29%) have written cyber security policies, and just one in ten (10%) have formal incident management processes. The guidance also highlights the importance of user education and training, although only 17 per cent of firms have had their staff undergo some form of cyber security training in the last 12 months.

- Relatively few companies (34%) have rules specifically around personal data encryption, which has been at the centre of various high-profile cyber security breaches in recent months.

Moreover, while most businesses set rules and controls *within* their organisations, just 13 per cent set minimum cyber security standards for their suppliers. This is particularly significant given that one of the main drivers of investment in cyber security raised in the qualitative interviews was because client organisations demanded it.

Cyber security breaches affect all kinds of businesses and the costs can be substantial

A quarter (24%) of all businesses detected one or more cyber security breaches in the last 12 months. This is substantially higher among medium firms (51%) and large firms (65%). Large firms are also more frequently targeted, with 25 per cent of those that experienced breaches having been breached at least once a month.

Across all size bands, by far and away the most common types of breaches experienced are viruses, spyware or malware (68%) and breaches involving impersonation of the organisation (32%).

Among the businesses that detected breaches, the estimated average cost of all breaches over the last 12 months is £3,480. This is much higher for large firms, at £36,500. The estimated average cost of the single most disruptive breach from the last 12 months is £2,620 across all businesses and £32,300 for large businesses.

However, the qualitative findings indicate that businesses face various barriers to accurate financial monitoring, and may therefore underestimate the costs they do and will incur from cyber security breaches. While businesses can easily account for direct costs, such as the time spent dealing with the breach, they often find it more difficult to account for the opportunity costs of lost staff time and to anticipate the multiple knock-on effects a breach can have across the business.

[3] See https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

[4] See https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary.

Moreover, behind these average cost estimates, there are a number of businesses that have experienced much higher costs. The most costly single breach captured in this survey is purported to have cost £3 million. Cases like this highlight that individual breaches or attacks can have large financial ramifications for a business, and they underpin the importance of businesses taking action to prevent and protect against these kinds of attacks.

Conclusions

The Cyber Security Breaches Survey shows definitively that cyber security is an issue that affects virtually all UK businesses, and one that most businesses treat as a high priority. It also highlights the major challenges, and potential solutions, around getting companies to better protect themselves against breaches:

- There is room for improvement across all businesses. Most can still introduce cyber security policies or documentation to formalise their approaches. Significant minorities also still need to implement basic security controls or user-access controls on their organisation's devices.

- Micro and small businesses, as well as those in less engaged sectors, may particularly benefit from being more aware of the range of Government support on cyber security such as the small business guidance[5], free online training[6], 10 Steps guidance and the Cyber Essentials scheme.

- Many medium and large businesses have more developed approaches, but could still do more around implementing data encryption rules, offering staff training and having formal incident management processes. Many could also harness their market power to raise standards among smaller suppliers.

Future surveys in this series will be able to examine progress on each of these areas and continue to inform businesses on how they can best deal with the evolving cyber security threat.

[5] See https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know.

[6] See https://www.gov.uk/government/collections/cyber-security-training-for-business.

1 Introduction

1.1 Background and objectives

The 2015 National Security Strategy confirmed cyber attacks to be one of the top threats to UK economic and national security.[7] Following the Strategic Defence and Security Review, the Government announced a £1.9 billion investment in cyber security over the next five years. This includes the creation of a National Cyber Security Centre in 2016, to be a major source of information and support for UK businesses on cyber security.

The investment underlines the Government's ongoing commitment to make the UK one of the safest places in the world to do business online. It also highlights the fast-evolving threat posed by cyber security attacks.

This research will help businesses to understand the nature and level of the threat they face, how they can best manage their own cyber security and what other similar businesses are doing. It also provides valuable evidence for the Government to shape future policy in this area. It covers:

- business awareness and attitudes towards cyber security
- approaches to cyber security, including estimates of business spending
- the nature and impact (including estimated costs) of cyber security breaches
- differences by size, sector and region.

1.2 Methodology

There were two strands to this research:[8]

- A random probability telephone survey of 1,008 UK businesses was undertaken from 30 November 2015 to 5 February 2016. The survey data have been weighted to be statistically representative of the UK business population by size and sector.[9]

- A total of 30 in-depth interviews were undertaken in January and February 2016 to follow up with businesses that had participated in the survey and gain further qualitative insights.

1.3 Interpretation of findings

How to interpret the survey data

The survey results are subject to margins of error, which vary with the size of the sample and the percentage figure concerned. For all percentage[10] results, subgroup differences by size, sector and region have been

[7] See https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

[8] More technical details and a copy of the questionnaire are available in the separately published Annex, available on the gov.uk website at: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016.

[9] Sole traders and public sector organisations were outside the scope of the study, so were excluded. In addition, businesses with no online presence were deemed ineligible, which meant that a small number of specific sectors (agriculture, forestry, fishing, mining and quarrying) were excluded.

highlighted only where statistically significant (at the 95% level of confidence).[11] There is a further guide to statistical reliability at the end of this report.

Analysis by business size splits the sample into micro businesses (2 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more).

Due to the relatively small sample sizes for certain sectors, these have been grouped with other similar sectors for more robust analysis. Groupings referred to across this report are as follows:

- administration or real estate
- construction or manufacturing
- education, health or social care
- entertainment, service or membership organisations
- finance or insurance
- food or hospitality
- information, communications or utilities
- professional, scientific or technical
- retail, wholesale or transport.

Region subgroup analysis for Wales and Northern Ireland has not been possible given small sample sizes.[12]

Where figures in charts do not add to 100% this is due to rounding of percentages or because the questions allow more than one response.

How to interpret the qualitative data

The qualitative findings offer more nuanced insights and case studies into how and why businesses hold attitudes or adopt behaviours with regards to cyber security. The findings reported here represent common themes emerging across multiple interviews. However, they are not intended to be statistically representative.

1.4 Acknowledgements

Ipsos MORI thanks all the businesses and individuals who agreed to participate in the survey development, survey fieldwork and follow-up in-depth interviews. We would also like to thank the Government's cyber security community for their input throughout the research process.

[10] Where subgroup mean scores are compared, the large variation in the data often means that these differences are not statistically significant – this is made clear throughout. However, looking at the pattern of mean scores across subgroups can still generate valuable insights in these instances.

[11] Subgroup differences highlighted are either those that emerge consistently across multiple questions or evidence a particular hypothesis (i.e. not every single statistically significant finding has been commented on).

[12] Similarly, small samples sizes for certain regions in England mean they are too small to be analysed individually and these were grouped as the North of England, the Midlands and the South of England (excluding London) for analysis purposes.

2 Profiling UK businesses

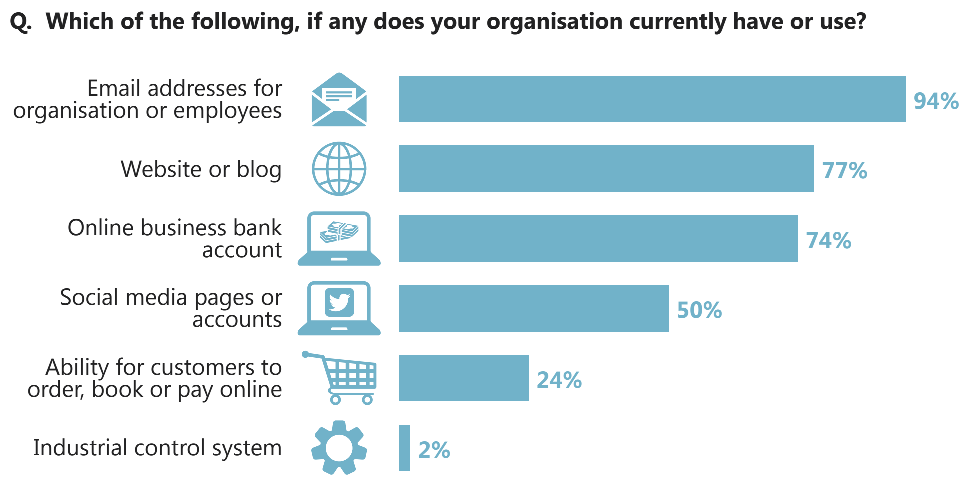
E-commerce has become much more important to UK businesses in recent years. Office for National Statistics data shows that in 2014, e-commerce sales were £573 billion across non-micro businesses, accounting for 20.1% of total business turnover. In 2008, these were £335 billion.[13] In this environment, it is worth reflecting on whether firms recognise the extent to which they operate online (and therefore see a need to be cyber secure).

This chapter lays out the extent to which UK businesses are online, and perceive themselves to be so. It also looks at their exposure to potential cyber security threats, including through the use of personal devices (e.g. smartphones) in the workplace or via cloud computing. This provides context for the different attitudes and approaches to cyber security evidenced in later chapters.

2.1 Online exposure

As can be seen in Figure 2.1, the vast majority of UK businesses employ online services in some form. Across all size bands, the large majority have group email addresses, a website or pages on social media sites, and online bank accounts. Online payment facilities for customers are also relatively common, and more prevalent in larger businesses (34% of medium businesses and 41% of large businesses have this function, versus 24% overall). Industrial control systems are, as might be expected, most prevalent among large firms (15%, which equates to over 900 large businesses).

Figure 2.1: Business use of online services



Base: 1,008 UK businesses

Which businesses consider themselves to be online businesses?

Around half (53%) of all businesses consider online services to be a core part of their offering, at least to some extent. As Figure 2.2 shows, 14 per cent say this is to a large extent.

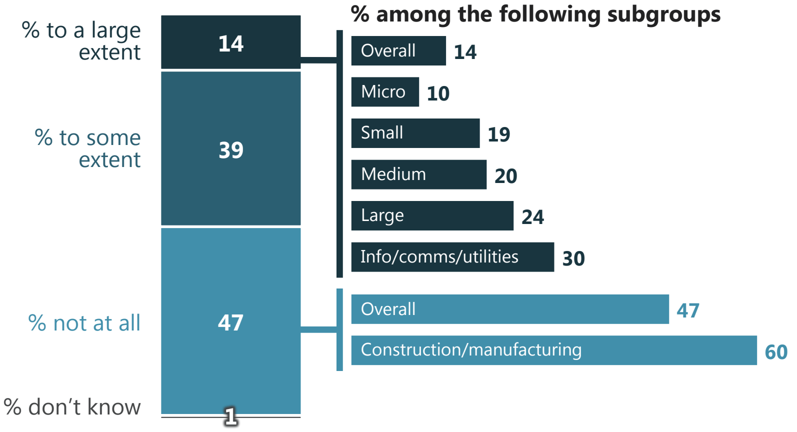
[13] See http://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/ecommerceandictactivity/2014.

While most businesses of all sizes use a variety of online services, the extent to which they consider themselves as online businesses varies considerably by size band. As Figure 2.2 indicates, micro firms are much less likely to view online services as core to their business than larger firms.

Information, communications or utility firms are more likely to consider themselves as online organisations than average. In contrast, six in ten construction or manufacturing firms (60%) think that online services are not at all core to their business offer, which may help contextualise the less developed approach to cyber security in this sector, evidenced in the rest of this report.

Figure 2.2: Businesses that consider online services as core to their business offer

Q. To what extent, if at all, are online services a core part of the goods and services your organisation provides?



Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms; 100 information, communications or utility firms; 177 construction or manufacturing firms

In particular, organisations are more likely to see themselves as online businesses once they take on online payment facilities. Among those that have these facilities, a quarter (26%) consider online services to be core to their offer to a large extent, with the vast majority saying this *at least* to some extent (86%). It is notable, however, that this leaves 14 per cent of businesses with online payment facilities that still think online services are not at all core to their business, and therefore may underestimate cyber security as an issue for them.

Which businesses feel exposed to cyber security risks?

The qualitative work highlights two factors beyond the size of the business and their use of online services that might make businesses feel more or less exposed to cyber security risks.

Firstly, the nature of the data that the business held was important. One participant in a video production firm discussed the sensitive nature of some of their client work, for example videos around new product launches or videos explaining the restructuring of a business to its staff. These could cause commercial or even emotional damage if leaked before publication. With this in mind, they were particularly concerned about the risk of emails being hacked, and had secure file transfer sites for clients to use.

By contrast, there was a sense from some participants that they would probably not be a target for serious attacks because they felt they had nothing worth stealing. Some specifically mentioned that this was because they were not a bank, or did not collect customers' financial details. Even when the firm had rules or policies in place around cyber security, these participants felt that there would typically not be any major consequences from losing these data, or at least no long-term consequences that the business could not rebound from.

"We don't hold financial information and detail. Obviously personal information, from the point of view of finding out people's details, but without financial details there's very little people can gain from us."
Medium business

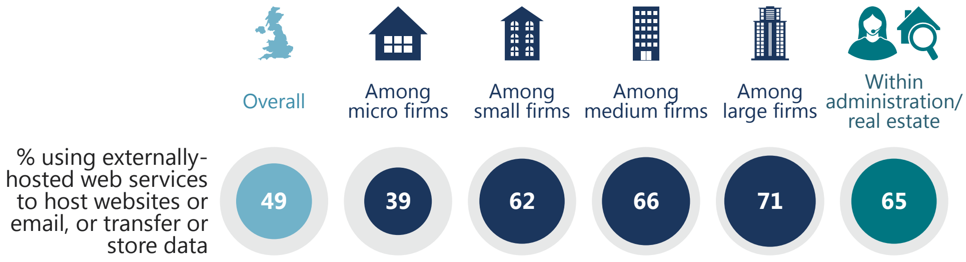
Secondly, in larger organisations, the online connectedness of the wider workforce could affect how they approached the issue. An example was a cleaning firm with a large overall workforce but only around 30 employees in the head office. As the wider workforce were offline in their work activities, the organisation had a less structured and documented approach to cyber security. Again, this might help to explain differences throughout this report found for sectors such as construction or manufacturing, and food or hospitality, which tend to be less engaged with cyber security.

While these kinds of businesses may feel cyber security is less relevant in terms of the data they handle, or the structure of their workforce, it is important that businesses take a broader view when assessing cyber security risks. Non-financial customer data are still valuable in an interconnected world where people often reuse the same passwords across sites and services. Moreover, risks are not only attached to the online activities of customers and staff, but also to human resources data, the smooth running of the business and any commercially-sensitive data held. Indeed, among firms that consider themselves to be offline businesses, one in five are still subject to cyber security breaches (see Chapter 5).

2.2 Cloud computing

Use of cloud computing is widespread among UK businesses, with around half (49%) using some sort of externally-hosted web service. As Figure 2.3 highlights, outside of micro firms a majority of businesses are using these services, and usage is particularly prevalent in the administration or real estate sectors.

Figure 2.3: Usage of externally-hosted web services



Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms; 136 administration or real estate firms

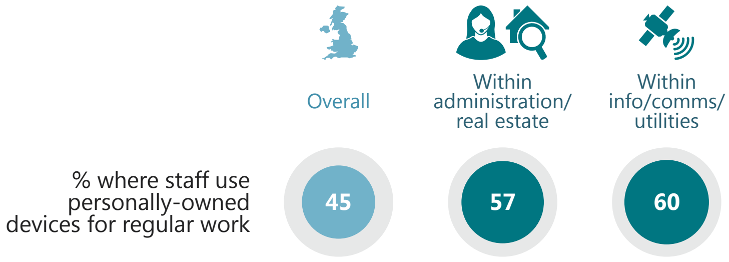
For the most part, businesses consider these services to be critical to their operations and most also consider at least some of the information stored on cloud servers to be confidential (although, as noted in Chapter 4, businesses are not always aware of how secure these data are). Among businesses that use these services:

- Two-thirds (67%) say these services are either very critical (33%) or fairly critical (34%) to their organisation. Almost half (47%) of all large businesses consider these services as very critical.
- Over half (55%) of all firms say at least some of the data stored on the cloud are commercially confidential, and this is greater for medium businesses (67%) and large businesses (65%).
- Half (48%) say that at least some of the cloud data are personal data about customers or employees, and this is consistent across size bands.

2.3 Use of personal devices

The cyber security risks of bringing your own device (BYOD) are unavoidable for over two-fifths (45%) of businesses, where the firm is aware of staff using personally-owned devices to carry out regular business-related activities. This is slightly higher among medium firms (50%) and large firms (54%). Figure 2.4 also shows sector differences, with BYOD being more prevalent in the administration or real estate sectors and information, communications or utility sectors.

Figure 2.4: Businesses where bringing your own device (BYOD) occurs



Bases: 1,008 UK businesses; 136 administration or real estate firms; 100 information, communications or utility firms

It is also noteworthy that firms that consider online services to a large extent to be core to their business are also those where BYOD is more prevalent than average (61%, versus 45% overall). This means that the businesses that are perhaps more at risk of BYOD-related cyber security breaches could also have the most to lose from a significant BYOD-related breach, given their strong reliance on e-commerce.

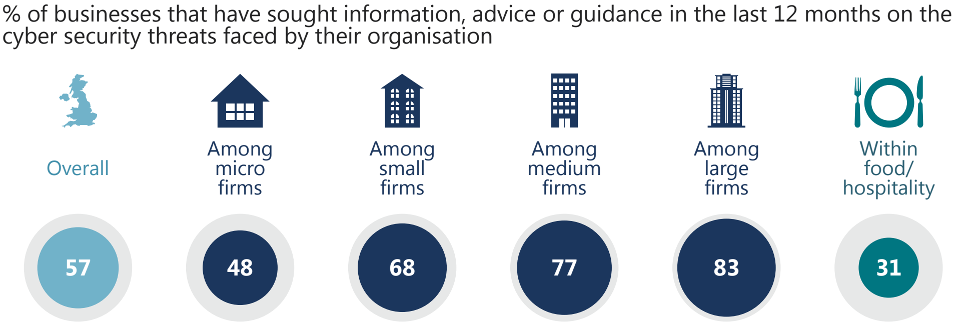
3 Business awareness and attitudes

This chapter looks at where businesses get information, advice or guidance about cyber security, and their perceptions of the support available. It also covers attitudes towards cyber security, and the factors underpinning these attitudes.

3.1 Sources of information

In the last 12 months, almost three-fifths (57%) of businesses have sought information, advice or guidance on the cyber security threats facing their organisations. As Figure 3.1 shows, this varies by size band, with smaller firms typically being less likely to have sought information. Businesses in the food or hospitality sectors are less likely than average to have looked for information.

Figure 3.1: Whether businesses have sought information, advice or guidance



Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms; 87 food or hospitality firms

Among businesses who treat cyber security as a low priority (covered later in this chapter), a quarter (24%) have nonetheless still sought information on the topic.

In terms of where people have sought information, the top specific unprompted mentions were external security or IT consultants (28%), Google or general online searching (9%) and security product vendors (6%). Overall, businesses are more likely to mention non-Government sources (34%) than Government ones (2%).

The qualitative research highlights the particular importance of outsourced cyber security providers as a source of information. In smaller businesses where there were no specialist IT or cyber security staff, participants noted that they would sense-check their actions with outsourced providers (where these were in place). For example, one micro business owner who felt he knew little about cyber security had double-checked with his new outsourced provider before allowing an employee to access the firm's Wi-Fi network. Participants felt that having a go-to provider in this way had made them more alert to cyber security and consequently made the business more secure.

Qualitative interviews also raised the importance of media stories around high-profile attacks in making businesses more aware of cyber security as an issue, and of the possible impact of a cyber security breach.

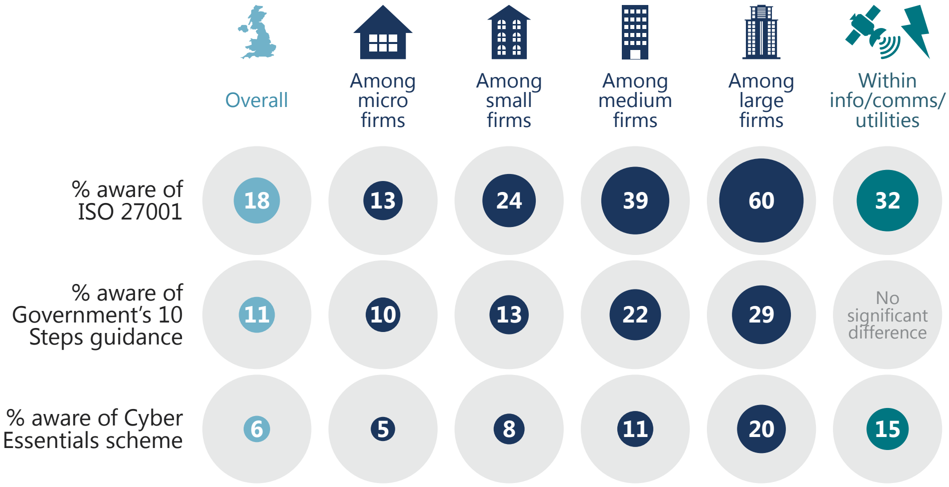
"We're all aware of what's going on in the media. We've all become aware that quite high-level criminal attacks via electronic means are becoming more frequent and more detrimental towards the business and the business image,"

Medium business

3.2 Awareness of Government initiatives and other standards

Across all businesses, accreditation schemes and standards relating to cyber security are not widely known, although there tends to be much higher awareness among large firms, as Figure 3.2 indicates.

Figure 3.2: Business awareness of cyber security initiatives and standards



	Overall	Among micro firms	Among small firms	Among medium firms	Among large firms	Within info/comms/ utilities
% aware of ISO 27001	18	13	24	39	60	32
% aware of Government's 10 Steps guidance	11	10	13	22	29	No significant difference
% aware of Cyber Essentials scheme	6	5	8	11	20	15

Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms; 100 information, communications or utility firms

In addition to information, communications or utility firms tending to be more aware of some of the initiatives and schemes asked about, education, health or social care firms are also more aware than the average about the international standard for Information Security Management, ISO 27001 (30%, versus 18% overall).

Demand for Government-led support

The qualitative research suggests that businesses perceive Government information and advice to be impartial and would therefore support the provision of additional guidance and help. For example, some participants were cautious of private companies trying to sell them software they did not fully understand, and raised the idea of the Government endorsing or accrediting certain software or outsourced cyber security providers as a way of guiding businesses towards the best of the private sector. It is worth noting that the Government's National Technical Authority for Information Assurance (CESG) does have schemes like this for certifying cyber security consultancies and Cyber Incident Response companies.

Lack of awareness of the range of information and advice available from the Government[14] might explain why some businesses have not accessed this support. Some micro business participants who were not aware of the

[14] See https://www.gov.uk/government/collections/cyber-security-guidance-for-business.

Government's 10 Steps guidance[15], the small business guide to cyber security[16] or the Cyber Essentials scheme (which includes five basic security controls for businesses to enact)[17] said they would have welcomed a similar checklist or starter pack when starting up their business.

Alongside this lack of awareness, there were also misperceptions about what was available. Some felt that Government advice was not as up-to-date as private sector advice online. This was because they were comparing the daily updates they got from threat intelligence services or antivirus providers to the less-frequently published guidance they saw on gov.uk (even if this guidance was still current).

There were also misperceptions that Government advice was not relevant to smaller businesses, or was only meant for businesses with more substantial cyber security risks. One participant highlighted that promoting gold-standard cyber security through the 10 Steps guidance came with the risk that smaller organisations would judge some of the steps to be too costly, and would therefore take no action, rather than implementing some basic minimum standards.

Again it is worth noting that the Government has recently addressed many of these challenges. Campaigns such as Cyber Streetwise[18] (aimed at smaller businesses) and the aforementioned small business guide to cyber security offer approaches tailored to micro and small businesses. The Cyber Essentials scheme is designed to be accessible to businesses of all sizes. It enables businesses to be certified for reaching good-practice basic standards, including a self-assessment approach (i.e. not necessarily advocating the gold standard or a resource-intensive approach to all businesses).

3.3 Importance of cyber security

Seven in ten businesses (69%) say cyber security is either a very high (33%) or fairly high (37%) priority for their organisation's senior management. Large businesses are also more likely to say this is a high priority area, with nine in ten (90%) saying this, as Figure 3.3 shows.

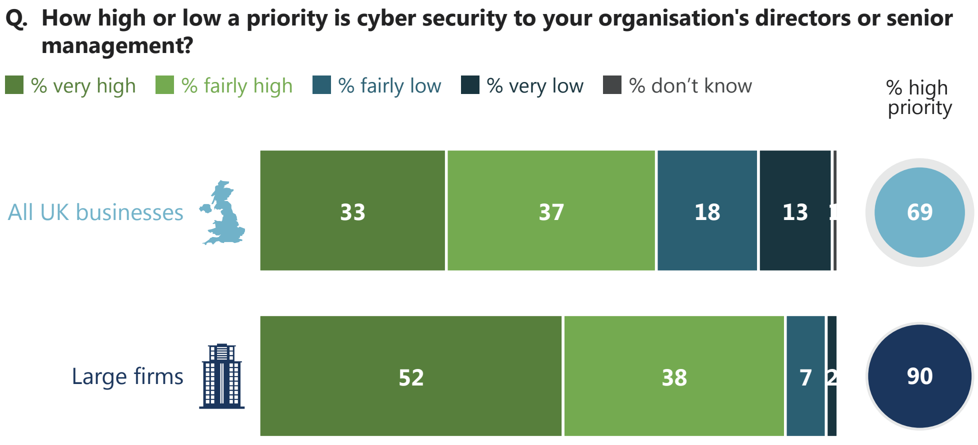
[15] See https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary.

[16] See https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know.

[17] See https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

[18] See https://www.cyberstreetwise.com/.

Figure 3.3: Whether senior managers consider cyber security a high priority



Bases: 1,008 UK businesses; 203 large firms

As might be expected, businesses that say online services are to a large extent core to their offering are more likely to consider cyber security a priority (89%, versus 69% overall).

Financial or insurance firms (90%) and administration or real estate firms (84%) are more likely than average (69%) to rate cyber security as a high priority for senior managers. In contrast, senior managers in entertainment, service or membership organisations (54%) and food or hospitality firms (52%) are less likely than others to see it as a high priority.

Irrespective of size or sector, the reason businesses most commonly cite for why cyber security is a low priority is that the topic is not relevant to them in general (47% of those who think it is a low priority for senior managers give this as the reason, unprompted). At the same time, medium or large businesses are more likely to raise lack of awareness and understanding of the topic as a reason for senior managers treating it as a low priority (23% mention this, versus 7% overall) and are more likely to mention the fact that cyber security is outsourced as a reason (24%, versus 2% overall).[19]

The latter difference around outsourcing suggests that there may be cases where senior managers in larger firms feel they have devolved responsibility for cyber security to external contractors and so no longer need to concern themselves with it internally. In these instances, businesses should consider who ultimately owns the risk and what the impact of a serious cyber attack would be on their business – often it is not possible to transfer reputational risk to a third party.

How often is senior management updated on cyber security?

A quarter (26%) of businesses report that their senior managers are *never* given an update on any actions taken around cyber security. This is even higher among entertainment, service or membership organisations (46%) and in the food or hospitality sectors (40%).

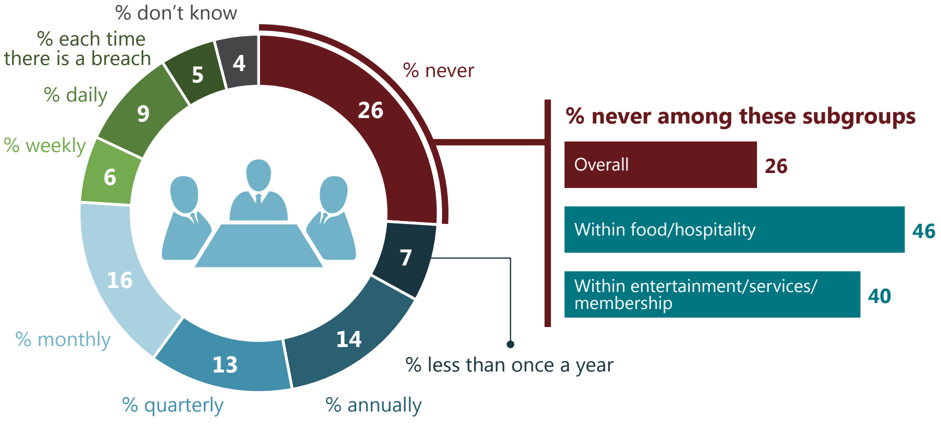
[19] Medium and large firms have been merged here due to the small effective sample size for large businesses alone.

Even among the businesses whose senior management are said to treat cyber security as a high priority, there are still 12 per cent where these senior managers are never updated on actions taken. This highlights that a minority of senior managers do not directly engage with cyber security and may be divorced from the actions that their organisations are taking, even if they think the topic is important for their business.

In terms of the more general trend, seen in Figure 3.4, there does not seem to be an accepted standard approach for briefing senior managers, with a range of organisations doing this all the way from less than once a year through to every time there is a breach.

Figure 3.4: Updates given to senior management on cyber security

Q. Approximately how often, if at all, are your organisation's directors or senior management given an update on any actions taken around cyber security?



Bases: 1,008 UK businesses; 74 food or hospitality firms; 87 entertainment, service or membership organisations

What makes cyber security important?

The qualitative research highlights various factors that can help make cyber security important:

- An increased focus on cyber security and the hiring of specialist staff often coincided with business growth and the development of governance structures (such as boards of directors). This seemed to be a particular factor for growing medium businesses. One participant highlighted how the newly-installed board of directors in their medium firm had started to professionalise the business to make it more compliant with information governance standards, as a way of securing future business.
- There were often key individuals within small and medium businesses who championed cyber security and argue the case to board members and Chief Executives. Some participants suggested that there might not be as much emphasis on the topic if they were not at the organisation.
- Related to this, having cyber security expertise among board members can also help others within the business to raise the issue. In some cases, participants said a lack of knowledge on the part of the board was one of the main barriers they faced to getting the firm to engage with cyber security.
- How the issue of cyber security is framed matters. As an IT issue, it often seemed to have less engagement from senior managers due to a lack of technical knowledge and understanding, and was

typically left to IT staff to deal with. By contrast, some participants framed it as a compliance or business performance issue to get the attention of senior managers. One micro business owner noted that he specifically placed cyber security alongside things like human resources and health and safety, as part of a package of things he thought a competent director would set up when starting up a business.

- In certain sectors there was a staff culture that emphasised confidentiality and good data management, and cyber security slotted well into these existing cultures. For example, within education, health or social care organisations, participants noted that there was already a strong recognition of client (i.e. student or patient) confidentiality and data protection law. Many staff in these organisations had previously worked in the public sector (e.g. the NHS), so brought good practices with them. In another case, a participant working in video production noted that staff in their sector were very IT-literate given the nature of their work, and that this gave them an appreciation for issues like encryption and password protection.

4 Approaches to cyber security

This chapter looks at how much businesses are investing in cyber security and what drives this level of investment. It then examines how firms broach the subject of cyber security with their staff, and the policies and procedures they have in place to identify and reduce risks.

4.1 Investment in cyber security

Levels of investment

Table 4.1 shows that two-thirds of all firms do have some level of cyber security spend. This varies, as might be expected, by size.[20] The typical micro or small business tends to spend a very small sum, just over what an annual subscription to antivirus or anti-malware software might cost, while the typical large firm spends at a level more akin to an individual's annual salary.

The data suggest that the variation in spending is much higher among large firms than others. This is likely to reflect the considerable sector differences shown later in Figure 4.1, with the largest firms having the capacity and choice to spend very large or relatively small amounts on cyber security.

Table 4.1: Average investment in cyber security in last financial year

	All businesses	Micro/small[21]	Medium	Large
Mean spend	£4,060	£2,290	£24,100	£269,000
Median spend	£150	£100	£3,900	£26,000
% spending £0	32%	32%	10%	6%
Base	812	385	278	149

If higher spending typically enabled businesses to better prevent breaches and deal with the ones they faced, there would be an expected inverse relationship between spending and costs. However, among micro and small firms, spending is *positively* correlated[22] with the estimated cost of breaches (see Chapter 5 for estimated costs). Among medium and large firms, there is no significant correlation, either positive or negative.

This highlights that the relationship between spending and costs is not straightforward. Among larger organisations, it could be that those that invest more are also better at identifying breaches, so there is not strictly an inverse relationship between spending and costs. Among smaller organisations, the positive relationship between spending and costs could suggest that spending is not always effective at preventing or

[20] Spending figures are presented to 3 significant figures or to the nearest whole number. The differences in mean figures presented here are statistically significant.

[21] Micro and small firms have been merged to make this analysis more statistically robust.

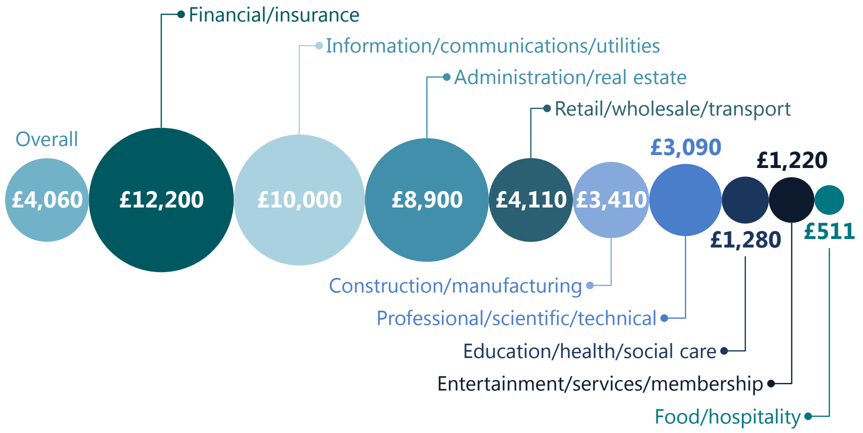
[22] Among micro and small firms that have had breaches in the last 12 months, the correlation coefficient for spending and the cost of these breaches is 0.38. This includes organisations that say they spend nothing on cyber security.

dealing with breaches. Equally it is an indicator that many smaller firms are investing in cyber security *after* suffering breaches, rather than as a proactive measure to prevent breaches.

Perhaps related to the concentration of large firms in London, spending levels tend to be greater there on average (mean spending of £5,470). Spending tends to be lower in Scotland (mean spending of £949).

As Figure 4.1 shows, spending does tend to be considerably higher in certain sectors, such as the financial or insurance sectors, information, communications or utilities, and administration or real estate. The pattern of spending does reflect the relatively high prioritisation of cyber security in these sectors (see section 3.3).

Figure 4.1: Average investment in cyber security in last financial year by sector grouping



Bases: 101 administration or real estate firms; 144 construction or manufacturing firms; 87 education, health or social care firms; 63 entertainment, service or membership organisations firms; 57 finance or insurance firms; 74 food or hospitality firms; 71 information, communications or utility firms; 84 professional, scientific or technical firms; 131 retail, wholesale or transport firms

Outsourcing cyber security

Just over two-fifths (44%) of businesses outsource their cyber security to external providers. This is more common among small firms (63%) and medium firms (66%) than among micro (31%) or large organisations (49%). It is also particularly common among administration or real estate businesses (64%).

The qualitative research helps explain the differences by size. Among micro firms, there was typically a more informal approach to cyber security and a relatively basic IT infrastructure, which meant that senior managers felt they could oversee cyber security themselves. Some small and medium firms employed an individual IT specialist but commented that, unlike large firms, they could not afford a whole team of specialist staff, and it was more cost-effective for them to outsource any maintenance that was beyond an individual staff member.

It is also important to note that when engaging outsourced providers, the prime consideration may not be cyber security. In some cases in the qualitative research, smaller businesses had chosen providers that could give them specific software solutions, such as an online payments system or a business server, and elements of cyber security were part of the maintenance package for this. Therefore, the level of security offered was generally not a deciding factor in choosing a suitable provider.

Two other criteria for choosing outsourced cyber security providers emerged in interviews:

- Trust based on an existing relationship with the provider was often important, in some cases overriding considerations of the technical capabilities of providers, which were assumed to be satisfactory. Some participants from small or medium firms noted that they had previously worked with their chosen providers in another capacity, so knew what they provided and trusted their work. They had since formalised that existing relationship to include cyber security. Some businesses may unwittingly be less secure because of their relatively informal approach to choosing a cyber security provider – businesses should also consider the credentials of cyber security providers when making this choice.

- The importance of outsourced providers understanding their impact on business performance was also raised. One large business noted how they wanted their outsourced provider to be a good cultural fit for their organisation, which meant understanding that if certain systems stopped working, this would stop a lorry from leaving their factory and have knock-on effects. This might also help to explain why fewer large firms outsource their cyber security overall.

Qualitative case study: choosing an outsourced cyber security provider

For the smallest businesses, decisions around outsourcing can be relatively informal. One micro business explained that they had initially tried to search online for a provider that could set up their online payments system, but had been put off by the jargon and the depth of the material they found. They took a recommendation from a friend and fellow small business owner, and went to see this in action. They were satisfied this system did what they required, so have since taken on the same provider, which now provides the organisation's cyber security.

Cyber security insurance

A recent Government report has indicated that the growth of the cyber security insurance market could spur better cyber security risk management, for example by encouraging businesses to implement Cyber Essentials or other minimum standards to benefit from lower insurance premiums, and by providing firms with better insight after breaches to help them avoid future claims.[23]

This research finds that around two-fifths (37%) say they have some form of cyber security insurance. This is significantly less common among micro firms (30%) than among small (47%), medium (48%) and large (40%) ones. It is also a more regular provision in education, health or social care organisations (52%), and is much less prevalent than average in construction or manufacturing firms (22%).

Here, the qualitative research suggests that cyber security insurance is often a bolt-on to broader insurance policies, such as professional indemnity insurance. In these cases, businesses had not sought out cyber security insurance specifically and there was a general lack of knowledge about what was covered within these policies. This finding chimes with previous insurance industry estimates, which suggest that in actual fact the

[23] Marsh (2015) UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk, HM Government (available online at: https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance)

overwhelming majority of businesses are not insured specifically against cyber security breaches.[24] In other words, while two-fifths think they are insured, they may not be covered if they have a breach.

In the qualitative interviews where businesses *had* specifically sought cyber security insurance, this was either done in response to breaches, so after costs had already been incurred, or it was done as a pre-requisite for achieving some form of accreditation.

Drivers of investment

When asked unprompted why in the main they invest in cyber security, the two most common reasons offered by businesses are around protecting company-owned data or intellectual property (44%) and protecting customer data (36%).

Relatively few organisations see cyber security mainly in terms of business continuity, with just 13 per cent saying one of their main reasons for investing is about keeping the business going, and just three per cent saying they invest to prevent downtime and outages. This does seem to be a bigger driver for larger businesses however, with two in ten (18% of medium firms and 19% of large firms) citing keeping the business going as one of their main reasons.

Cyber security is also largely *not* viewed as a compliance issue, with just five per cent saying compliance with laws and regulations was one of the main reasons behind their investment. This was slightly higher among small organisations (9%).

Medium and large firms are also less likely than average to have invested in cyber security to protect against viruses (just 3% and 2% respectively mention this, compared with 8% overall), suggesting this is more of a concern among smaller businesses. This reflects the qualitative research, in which interviews with smaller businesses were often framed more around antivirus protection and keeping software up to date, and less around broader issues such as data handling or encryption.

The qualitative research also provides important insights around why investments were made:

- Participants mentioned various cautionary tales that had prompted them to spend money in this area. These included breaches their own organisation had suffered, incidents that they were aware of among suppliers or competitors and high-profile breaches covered in the media.
- As with decisions to engage outsourced providers, spending on cyber security more generally was often not for its own sake, but driven by a business need. So businesses that required an online payments system would put this in place and then have to invest in the maintenance and security of the system. Reframing cyber security in terms of these business needs (e.g. ensuring that online payments do not crash) might therefore encourage smaller businesses to invest.

[24] In the Government's 2015 report on The Role of Insurance in Managing and Mitigating the Risk, estimates based on actual policies placed by insurers suggest that around two per cent of large firms and close to zero smaller firms have specific cyber security insurance.

- In certain sectors such as the financial or insurance sector, and education, health or social care sectors, investments were often made in order to gain access to markets or even certain clients (such as the NHS) that demanded particular standards. This particularly highlights how big clients can help drive behaviour change among businesses.

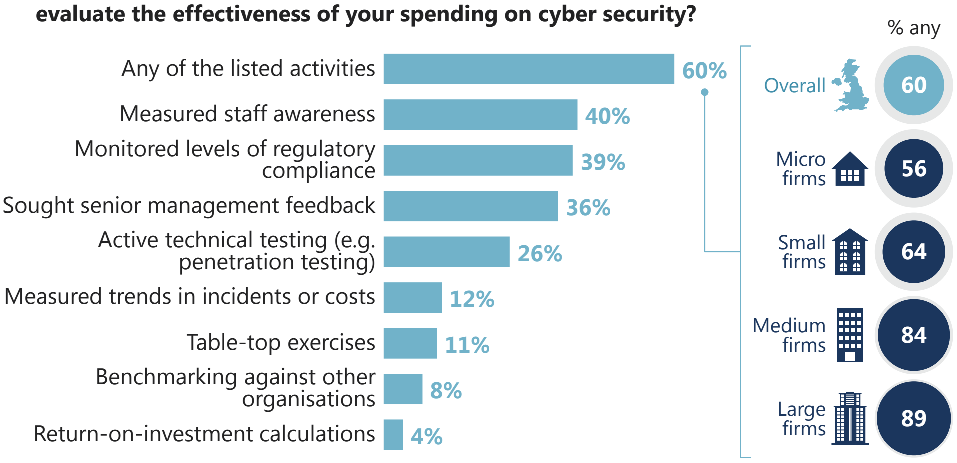
Justifying investments

Of those investing, three-fifths (60%) have formally evaluated their spending on cyber security in one of the ways listed in Figure 4.2. The most common actions centre on canvassing staff or senior management, or monitoring compliance. More sophisticated testing or benchmarking tends to be less common. Actual return-on-investment calculations are especially uncommon, with just four per cent of businesses having done these.

Large and medium firms are more likely to have carried out each of these specific evaluation activities than average. Nonetheless, even among these organisations, only a minority have measured trends, or carried out table-top exercises, benchmarking or return-on-investment calculations.

Figure 4.2: Ways in which businesses have evaluated cyber security spending

Q. In the last 12 months, which of the following things, if any, have you done to formally evaluate the effectiveness of your spending on cyber security?



Bases: 668 investing in cyber security; 155 micro firms; 113 small firms; 255 medium firms; 145 large firms

There are differences in approaches by sector. Firms in the professional, scientific or technical sectors are more likely than average to have monitored regulatory compliance (55%, versus 39% overall), sought senior manager feedback (52% versus 36%) and carried out table-top exercises (31% versus 11%) – the former difference perhaps reflects a relatively strong emphasis on compliance in areas such as accountancy, tax and law, which form part of this sector grouping. Information, communications or utility firms are more likely than average to have undertaken return-on-investment calculations (13% versus 4%).

The qualitative research highlights that a more technical approach to evaluating spending or even measuring the financial return on investment in isolation may not be the best way to engage senior managers. Participants indicated that senior managers often had an unsophisticated understanding of cyber security and would not necessarily appreciate risks until they were visible, for example if the email server stopped working or spyware started getting through. For this reason, participants thought it was often better to explain the potential real-life consequences and worst-case scenarios that might result from a breach, rather than try to put across a cost-benefit analysis.

"I always give them the worst case scenario, in the sense that I say, 'if we have a major breach then you're looking at being offline for at least 24 hours while we spin up a new server, so that's 24 hours of all of our salaries.'"
Medium business

4.2 Staff approaches

Who is responsible for cyber security?

In total, one-third (34%) of businesses employ staff whose job role specifically includes information security or governance. This is much higher among medium firms (60%) and large firms (75%), the majority of which have someone in this role. Staff with a cyber security-related remit are also much more of a feature in the financial or insurance sectors (60%) and the education, health or social care sectors (52%), perhaps reflecting the emphasis on compliance in these sectors found in the qualitative work.

The qualitative interviews also illustrate the difficulties faced by smaller organisations that do not employ specialist IT or cyber security staff. In these smaller organisations, cyber security typically sat alongside IT and was in many cases left to the IT enthusiasts within the business. This could lead to a sense of assumed technical knowledge, where the person left in charge would implement what they could from what they knew, but would not necessarily know much about cyber security (as opposed to IT in general).

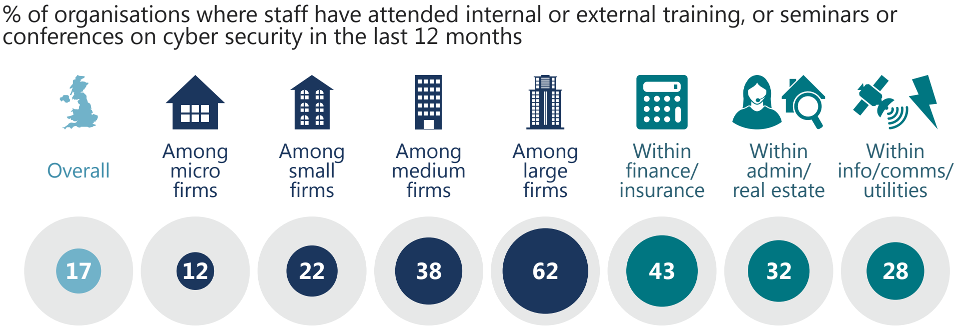
Staff training

Overall just under a fifth (17%) of businesses have had their staff attend some form of cyber security training in the last 12 months. This breaks down as 12 per cent of all businesses providing training internal to the organisation, six per cent providing external training, and six per cent where staff attended related seminars or conferences. Of all businesses, seven per cent (30% among large businesses) include this training as part of an induction process, and eight per cent (39% among large businesses) offer it as a regular training activity.[25]

As Figure 4.3 shows, this ranges considerably by size, with training being provided in the majority of large firms, and much more commonplace in the financial or insurance, administration or real estate and information, communications or utility sectors. Training is less prevalent among the retail, wholesale or transport sectors (9%, versus 17% overall) and the construction or manufacturing sectors (8%).

[25] While "training" was self-defined by respondents at this question, it is most likely in the wording of the question to be off-the-job training that staff attend away from their day-to-day work.

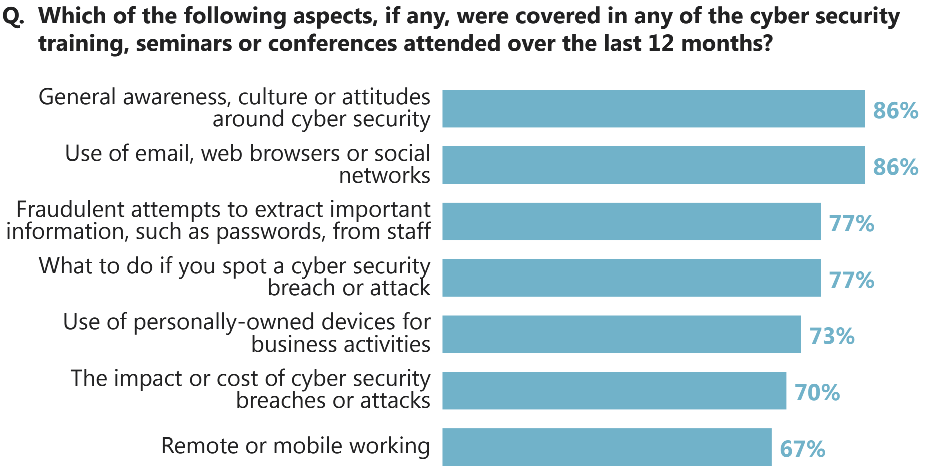
Figure 4.3: Businesses where staff have had cyber security training in the last 12 months



Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms; 75 financial or insurance firms; 136 administration or real estate firms; 100 information, communications or utility firms

Figure 4.4 highlights that a range of areas are typically covered in training. Three-fifths of the businesses that offer training cover at least six of the seven areas mentioned, and around a third (36%) cover them all.

Figure 4.4: Areas covered by cyber security training



Base: 355 that have offered cyber security training, seminars or conferences in the last 12 months

Businesses should note that the Government offers free online training courses on cyber security for businesses and professionals.[26] Businesses can also use the aforementioned Cyber Essentials scheme support, and the tailored guidance for larger and smaller businesses on the gov.uk website to assist in staff training.

4.3 Governance and planning

Formal policies and documentation

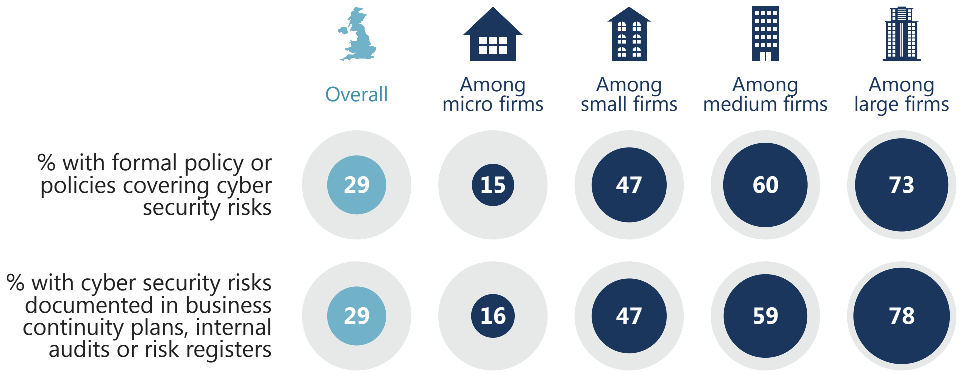
Looking at Figure 4.5, it is clear that the vast majority of micro firms and around half of all small firms do not tend to formalise their approach to cyber security in writing, through policies or other documentation. By

[26] See https://www.gov.uk/government/collections/cyber-security-training-for-business.

contrast, around six in ten medium sized businesses and over seven in ten large businesses do this, although it is notable that a quarter of large firms still do *not* have any policies around cyber security.

The qualitative work suggests that the responsible individuals in smaller organisations might feel comfortable with their more informal approach to cyber security. One micro business participant highlighted that the organisation was small enough for them to be able to monitor staff activity without needing a written policy, and they also did not want to be seen to actively police what staff could and could not do, because this would interfere with the friendly atmosphere that they wanted in their office.

Figure 4.5: Whether businesses have formal policies or document cyber security risks



Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms

Businesses in the financial or insurance sectors (49%) and the education, health or social care sectors (49%) are more likely than the average (29%) to have formal policies. Construction or manufacturing firms (15%) are among the least likely to have such policies in place.

The same sectors that have cyber security policies are also more likely to have documented their cyber security risks elsewhere – compared with an average of three in ten (29%):

- Just over half (53%) of all financial or insurance firms have documented risks.
- Around half of all education, health or social care firms (47%) have done so.
- Over two-fifths of professional, scientific or technical firms (44%) have done so.

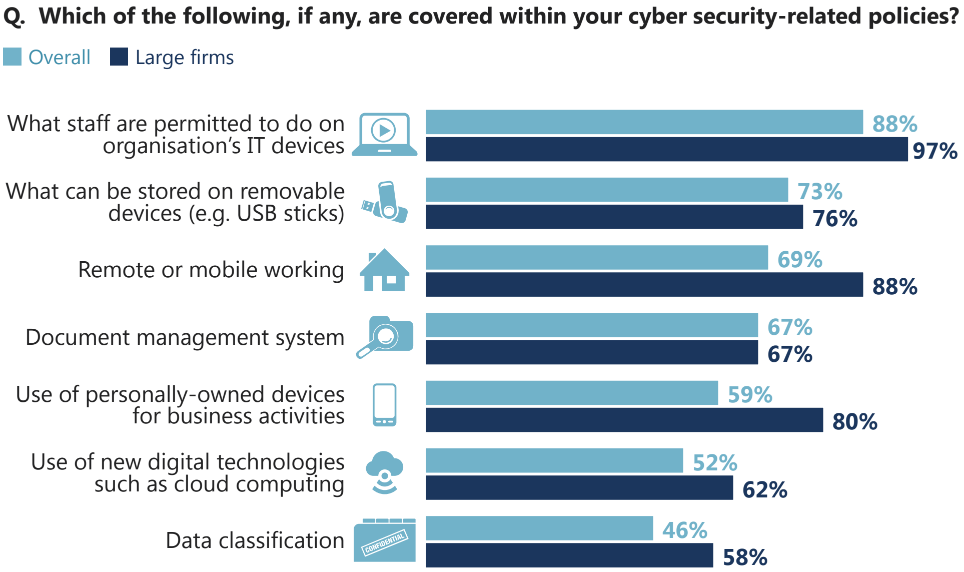
The fact that education, health or social care firms tend to have far more formalised approaches to cyber security (and are also more likely to have insurance and specialist staff) may reflect the potential cultural difference found in the qualitative research, with client confidentiality being taken especially seriously in education, health and care settings (see section 3.3).

What is covered in policies?

As can be seen in Figure 4.6, where they are in place, cyber security policies most commonly cover how staff can use the business's IT devices. There is typically less coverage of risks potentially occurring outside company-owned devices or environments, for example when it comes to removable devices, personally-owned devices, working from home or cloud computing.

Policies within large firms are notably more comprehensive, particularly in covering remote working and the use of personally-owned devices. However, even among large firms, the use of cloud computing or data classification is still not covered in around two-fifths of cases.

Figure 4.6: Most common features of cyber security policies



Bases: 498 with cyber security policies; 150 large firms

It is worth noting that even among businesses where staff regularly use personally-owned devices for business reasons, three in ten (29%) of those who have policies do *not* have this aspect covered in their policies.

Similarly, within businesses that use cloud-based servers and have cyber security policies, it is still only in six in ten (58%) cases that the policy covers cloud computing.

The qualitative research highlights good examples and ideas for how small and medium businesses might go about formulating policies or documentation. One participant raised the fact that there were many free resources available to organisations, such as the Information Commissioner's Office self-assessment toolkit.[27] Others mentioned that they had adapted their own policies from those of larger public sectors organisations (such as NHS Trusts) which published them on their websites.

Board responsibilities

As the qualitative research has shown, having board-level engagement with cyber security is important in ensuring the issue is taken seriously across the business. The Government's 10 Steps guidance, guidance for non-executive directors[28] and upcoming National Cyber Security Centre are all designed to support board members to engage with the topic.

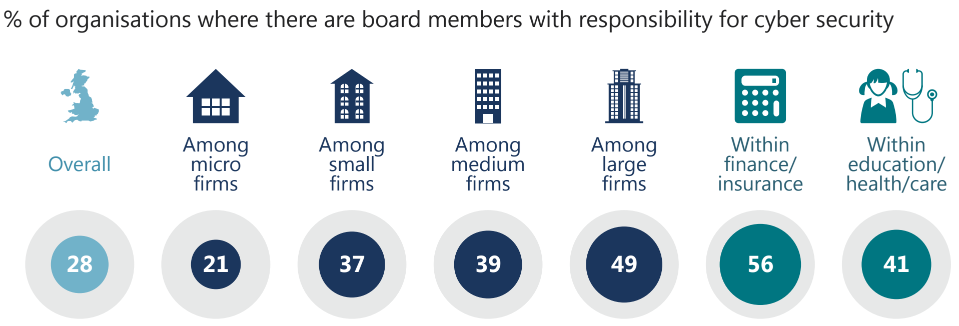
[27] See https://ico.org.uk/for-organisations/improve-your-practices/data-protection-self-assessment-toolkit/.

[28] See https://www.gov.uk/government/publications/cyber-security-balancing-risk-and-reward-with-confidence.

Across all size bands, having cyber security responsibility at a board level is still relatively uncommon, especially in comparison to the proportion that have cyber security documentation and treat it as a high priority. Overall, three in ten (28%) businesses have cyber security represented within their senior management boards, and this is more typical (though not widespread) among medium and large firms than among smaller firms, as Figure 4.7 shows. This may be a particularly significant issue for medium firms, with the qualitative research having highlighted the importance of having cyber security knowledge and understanding at the board level for these businesses, to help prioritise the issue (see section 3.3).

Once again, in line with their more formalised approaches to cyber security, the sectors more likely than average to have board members responsible for cyber security are finance or insurance, and education, health or social care.

Figure 4.7: Whether businesses have board members with responsibility for cyber security



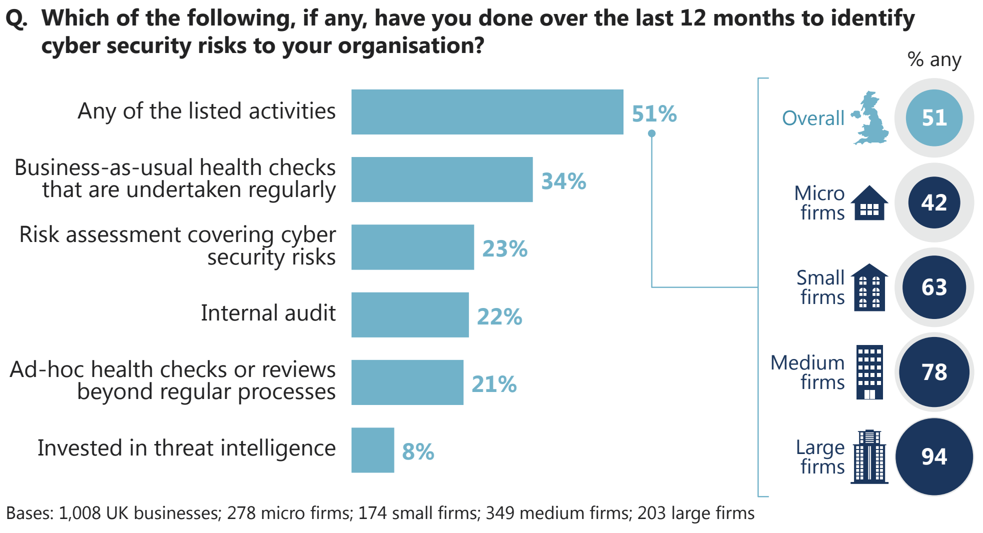
Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms; 75 financial or insurance firms; 107 education, health or social care firms

4.4 Risk management

Identifying and preventing risks

Figure 4.8 shows that half (51%) of all businesses, and the overwhelming majority (94%) of large businesses have taken some form of action to identify cyber security risks. The most common action involves undertaking regular checks, while ad hoc checks or audits are less common, and investing in threat intelligence is particularly uncommon (8% overall, and 34% among large firms).

Figure 4.8: Ways in which businesses have identified cyber security risks in the last 12 months



Information, communications or utility firms (73%) and professional, scientific or technical firms (67%) are more likely than the average (51%) to have undertaken any activities to identify risks.

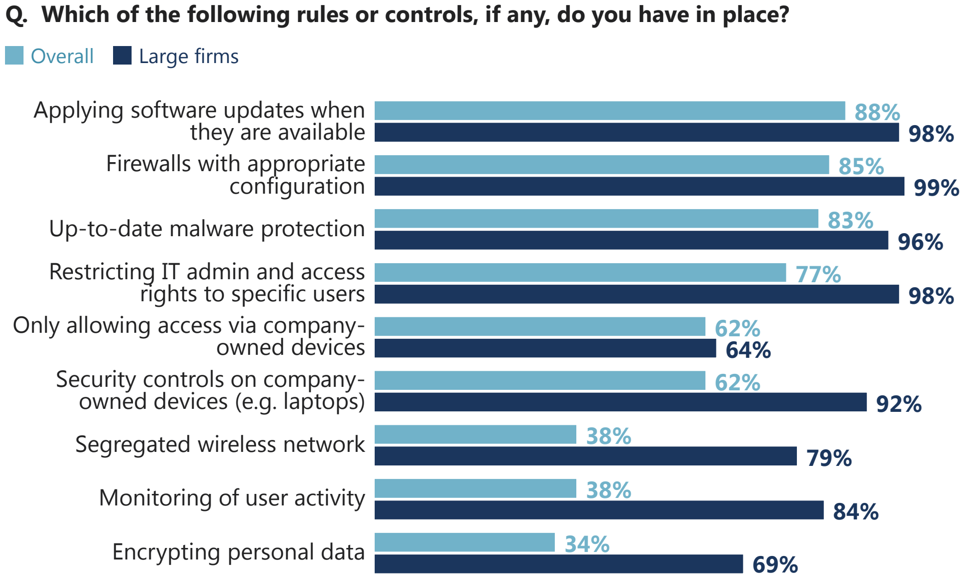
As Figure 4.9 shows, the overwhelming majority of businesses across all size bands say they regularly update their software and malware protections, and have configured firewalls, suggesting that these are seen as minimum standards in most cases. The majority of organisations also have rules restricting IT access or interactions, restricting access to company-owned devices (although, as discussed later, this may not always be enforced) and the placing of security controls on devices, although these are typically less common.

Other types of controls around wireless networks, user monitoring and encryption are atypical overall, although the majority of large organisations still implement these. However, it is notable that three in ten large firms (31%) do not have rules around personal data encryption, which has been at the centre of various high-profile cyber security breaches in recent months. Even among those organisations who say cyber security is a high priority, only four in ten (42%) have rules around encrypting personal data.

Encryption may therefore be an area where many organisations can implement stronger controls. The Information Commissioner's Office has recently published guidance about encryption, with recommendations for how it can be used effectively. Firms that hold sensitive personal information can consult this guidance.[29]

[29] See https://ico.org.uk/for-organisations/encryption/.

Figure 4.9: Rules or controls that businesses have implemented



Bases: 1,008 UK businesses; 203 large firms

While certain minimum rules prevail across businesses of all sizes, two sectors stand out as potentially lagging behind even on these commonly adopted rules:

- Food or hospitality firms are less likely than average to apply software updates when available (79%, versus 88% overall), have firewalls with appropriate configurations (75% versus 85%) or have updated malware protection (67% versus 83%).
- Entertainment and membership organisations are also less likely to apply software updates (79%), have firewalls with appropriate configurations (70%) or have up-to-date malware protection (63%).

It is worth noting that with the high prevalence of bringing your own device (BYOD) – staff in over two-fifths (45%) of businesses do this (see section 2.3) – enforcement of rules around only allowing access via company-owned devices may be challenging for businesses. The survey shows that even among those who say they only allow access through company devices, almost two-fifths (37%) still say staff use personally-owned devices to carry out their work regularly.

Dealing with third-party suppliers or contractors

The qualitative research highlights the cyber security challenges faced by medium and large businesses that work with smaller contractors. Some of these businesses had implemented stringent controls within their own organisations, but needed to work with smaller contractors or suppliers that would not necessarily have the same controls. Participants in medium businesses raised this as an issue that had become more apparent to them as they had improved their own cyber security approach.

On the other hand, it was also apparent that medium and larger businesses had significant market power to potentially set minimum standards for their suppliers, since these suppliers could be locked out of the market or suffer reputational damage if they did not meet these conditions.

"We build into the contract the ability to do a physical audit on the supplier premises … It would be a huge embarrassment for them to compromise our data."
Large business

Qualitative case study: raising cyber security among suppliers

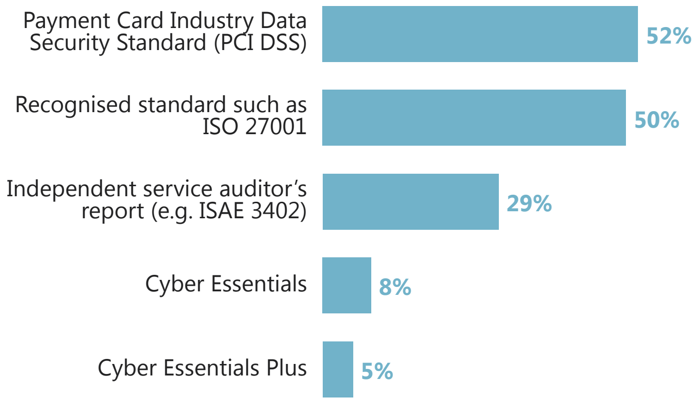
A children's social care provider was concerned about possible breaches emanating from smaller suppliers whose standards may be less stringent than their own. They relied on being able to subcontract some emergency care social workers when their in-house carers were fully booked, and were aware that some of the organisations they have worked with were not information governance-compliant – a requirement they were now writing into supplier contracts. It is these smaller businesses, they felt, that needed more Government help and support.

The survey shows that, while most businesses have rules or controls for their own operations (and most medium or large organisations have formally documented their approaches), all size bands are much less likely to set minimum standards for their suppliers. Just 13 per cent overall do this, rising to a quarter (25%) of medium firms and a third (34%) of large firms. Once again, this practice tends to be more common in the finance or insurance sectors (25%) and education, health or social care sectors (25%).

In this 13 per cent of cases, the most common requirements placed on suppliers are to adhere to a recognised international standard. A small number of businesses are using the Government-backed Cyber Essentials scheme with suppliers at present, as shown in Figure 4.10. Since October 2014 the Government has required its own supply chain to implement Cyber Essentials and, going forwards, this may influence others to follow suit.

Figure 4.10: Most commonly required cyber security standards for suppliers

Q. Which of the following, if any, do you require your suppliers to have or adhere to?



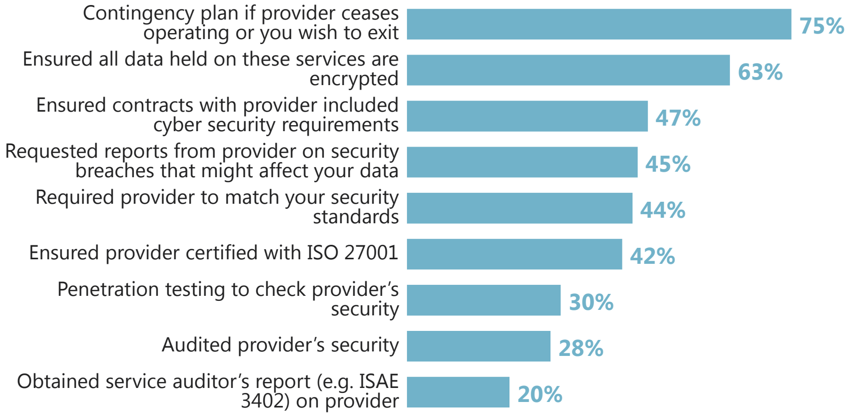
Base: 241 with supplier standards

Even among those using externally-hosted web services, such as cloud computing, only two in ten (20%) validate the suppliers of these services. Again this is higher among medium (33%) and large (43%) organisations using these cloud services, but still not a majority practice. It is also more commonplace for firms from professional, scientific or technical sectors (45%) to do this.

As Figure 4.11 shows, the most common actions taken to validate providers of these services are ensuring contingency plans are in place and confirming that data are encrypted. More in-depth actions such as carrying out audits, amending contracts or requesting fuller reports are also undertaken, though they are less common.

Figure 4.11: Most common ways of validating providers of externally-hosted web services

Q. Which of the following, if any, have you done in the last 12 months to test or validate the security of providers of online services?



Base: 190 that have validated security of external online service providers

4.5 Implementing Government initiatives and other standards

Cyber Essentials

The Government-backed Cyber Essentials scheme enables businesses to be independently certified for having met a good-practice standard in their cyber security. It requires businesses to enact basic technical controls across five areas: boundary firewalls and internet gateways, secure configurations, user access controls, malware protection, and patch management. The survey findings show that half of all firms (48%), including the vast majority of medium (76%) and large firms (87%), already say they have controls in these areas, but most may not currently realise they can be certified for this.[30]

Reflecting the relatively low awareness at present of the Cyber Essentials scheme (see section 3.2) only two per cent of all businesses recognise having implemented the Cyber Essentials standard across their business. A higher proportion (10%) of large organisations recognise that they have implemented the standard, although the scheme is relevant for businesses of all sizes. Information, communications or utility firms are also somewhat more likely to recognise having adopted this standard (8%, versus 2% overall).

[30] In the survey, the answers taken to indicate these controls are: firewalls with appropriate configuration, security controls on company-owned devices, restricting IT admin and access rights to specific users, up-to-date malware protection, and applying software updates when they are available.

10 Steps

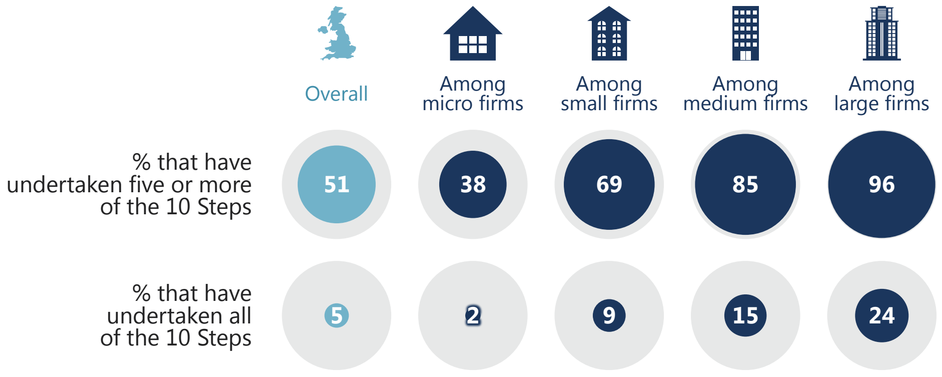
The Government's 10 Steps guidance is intended to outline the practical steps that organisations can take to improve their cyber security. These steps are covered individually across this report. Table 4.2 brings them together and again shows that, while most businesses have certain technical controls, fewer have taken a more sophisticated approach in terms of senior-level risk management, user education and incident management.

Table 4.2: Proportion of businesses undertaking each of the 10 Steps

	Step description – and how derived from the survey	**%**
1	Information risk management regime – formal cyber security policies or other documentation and the board are kept updated on actions taken	34%
2	Secure configuration – organisation applies software updates when they are available	88%
3	Network security – firewalls with appropriate configuration	86%
4	Managing user privileges – restricting IT admin and access rights to specific users	77%
5	User education and awareness – staff training at induction or on a regular basis, or formal policy covers what staff are permitted to do on the organisation's IT devices	28%
6	Incident management – formal incident management plan in place	10%
7	Malware protection – up-to-date malware protection in place	83%
8	Monitoring – monitoring of user activity or regular health checks to identify cyber security risks	51%
9	Removable media controls – formal policy covers what can be stored on removable devices	21%
10	Home and mobile working – formal policy covers remote or mobile working	20%

As Figure 4.12 highlights, half (51%) of all businesses have undertaken five or more of these steps, and larger businesses tend to have made more progress in this. Nonetheless, most businesses could still benefit from reviewing this guidance, as very few have made progress on *all* the steps. Through its upcoming National Cyber Security Centre, the Government will continue to support organisations to implement these steps wherever necessary.

Figure 4.12: Progress in undertaking the 10 Steps by size of business



Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms

ISO 27001

Implementation of the international standard for Information Security Management, ISO 27001, is also relatively uncommon. Among those who are aware of this standard, a quarter (26%) have implemented it and a further quarter (24%) are intending to do so in the future. This is consistent across size bands. Across all businesses (i.e. not just those who are aware of the standard), this equates to five per cent having implemented ISO 27001 and four per cent intending to do so.

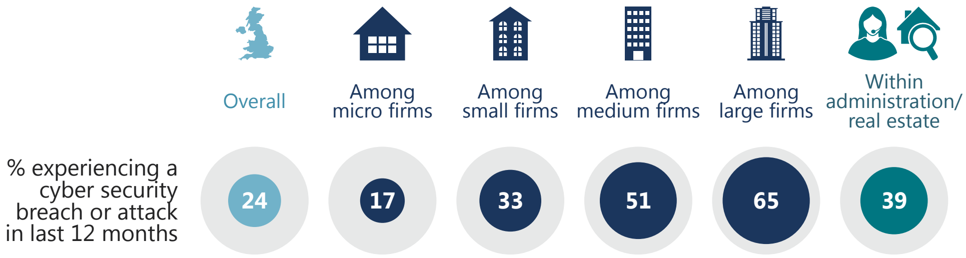
5 Incidence and impact of breaches

This chapter provides measures of the nature, level and impact of breaches incurred by businesses, including estimates of the total economic cost. The survey aims to account for all types of breaches that a firm might face (although it can only, of course, measure the breaches that have been identified), and also drills down into the most disruptive breaches.

5.1 Experience of breaches

As per Figure 5.1, a quarter (24%) of all businesses have experienced one or more cyber security breaches in the last 12 months. As the size of a firm increases, so too does the incidence of breaches, with two-thirds (65%) of large firms having faced a breach over this period. Breaches are also more common among administration or real estate firms (39%).

Figure 5.1: Proportion of businesses that have had breaches in last 12 months



Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms; 136 administration or real estate firms

Among the businesses that suggest cyber security is a low priority for them, the incidence of breaches does tend to be slightly lower on average, with 14 per cent having detected a breach in the last 12 months (compared with 24% overall).

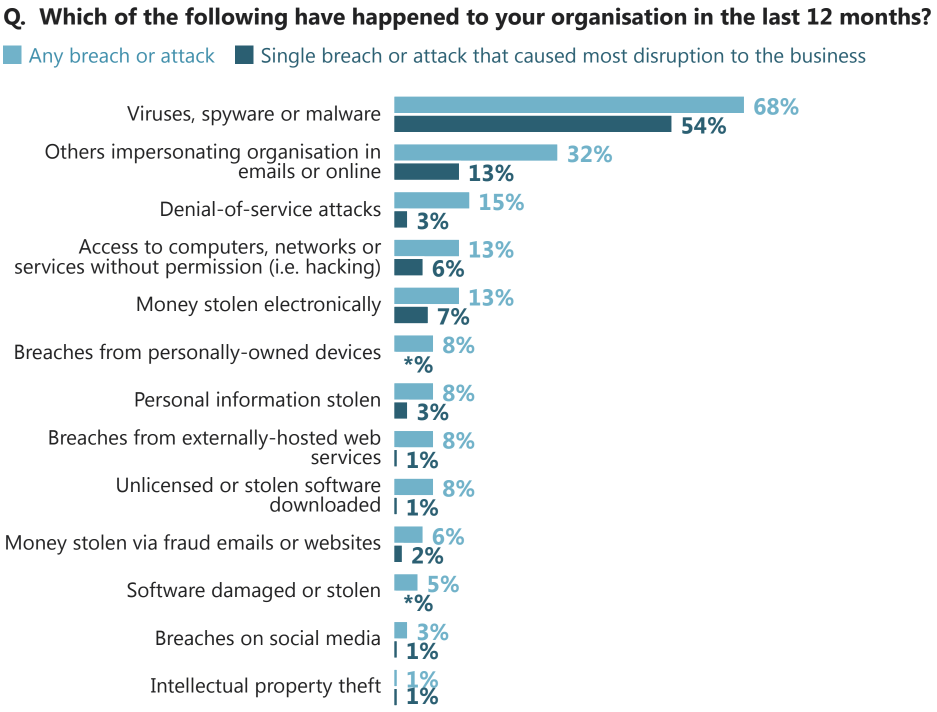
Among those who say online services are not at all core to their business offer, breaches are also less prevalent but it is of note that 18% per cent have still detected a breach in this period. This perhaps highlights that a minority of firms mistakenly think that cyber security is not relevant to them but are almost equally susceptible to breaches as the average.

Businesses that invest in cyber security are more likely to have experienced breaches than those who do not spend anything on it (33% versus 8%). This may in part reflect the qualitative finding that having a breach is often a catalyst for investment. At the same time, it could also be that businesses investing in cyber security are better at identifying breaches, since they are more engaged with the topic.

Types of breaches experienced

By far and away the most common types of breaches experienced are viruses, spyware or malware (68%) and impersonation of the organisation (32%). Viruses, spyware and malware are also typically the types of breaches that cause most disruption to businesses, which Figure 5.2 shows.

Figure 5.2: Types of breach suffered among those who have had breaches



Base: 428 that had a breach or attack in the last 12 months
* denotes a percentage less than one per cent but greater than zero.

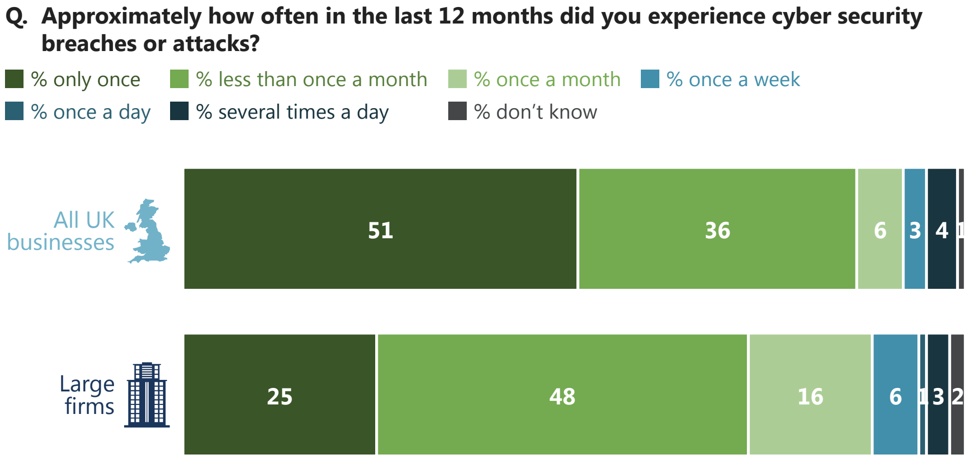
Certain sectors more typically experienced certain types of breaches:

- Administration or real estate firms were more likely to suffer viruses, spyware or malware (77%, versus 68% overall). They were also more likely to have money stolen electronically (26% versus 13%) and via fraudulent emails or websites (18% versus 6%).
- Information, communications or utility firms were more likely to have breaches relating to personally-owned devices (19% versus 8%). This is potentially linked to the fact that bringing your own device (BYOD) is more prevalent in this sector.
- Businesses in the financial or insurance sectors were more likely to suffer from impersonation in emails or online (60% versus 32%).

Extent of breaches experienced

Across all businesses that experienced breaches, half (51%) have only experienced breaches on one occasion. As Figure 5.3 shows however, large organisations are more likely to have been struck more often, with 25 per cent of those that have had breaches experiencing these at least once a month.

Figure 5.3: Frequency of breaches experienced in last 12 months



Bases: 428 that had a breach or attack in the last 12 months; 138 large firms

Table 5.1[31] shows that the mean number of breaches is substantially higher than the median number. What this indicates is that the majority of businesses only experience one or, at most, a handful of breaches in the space of a year, but a certain minority of businesses across all size bands are experiencing several dozens of breaches in this timeframe.

The volume of breaches tends to vary much more for medium firms than for larger or smaller ones.

Table 5.1: Average number of breaches among those that had any breaches in last 12 months

	All businesses	Micro/small[32]	Medium	Large
Mean number	66	59	189	66
Median number	1	1	2	5
Base	418	110	176	132

5.2 How are businesses affected?

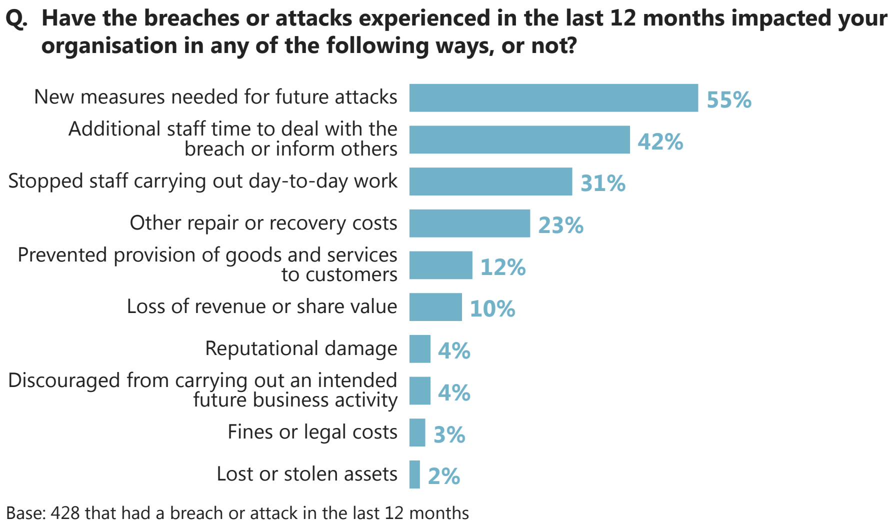
Nature of the impact

The main impacts that businesses say they have suffered when they have had breaches are having to implement protections against future breaches, staff time taken up both in dealing with a breach and through not being able to work as usual, and other repair costs (with businesses facing one or more of these impacts in at least a quarter of cases). Other impacts such as loss of revenue or reputational damage are less commonly identified. Figure 5.4 shows the full list of impacts covered in the survey.

[31] Figures are presented to 3 significant figures or to the nearest whole number. It should be noted that while the mean figure differences by size band are large, they are not statistically significant due to large variation within the data. Nevertheless, looking at the broad pattern by size still provides valuable insights.

[32] Micro and small firms have been merged to make this analysis more statistically robust.

Figure 5.4: Impact of breaches experienced in last 12 months



The ranking shown in Figure 5.4 is similar across size bands, though micro firms are more likely to say that they have suffered a loss of revenue due to breaches (18%, versus 10% overall).

The organisations that say online services are core to their business to a large extent are more likely to cite reputational damage from breaches (14%, versus 4% overall).

While most breaches are not seen to result in reputational damage, the qualitative research indicates that the *threat* of reputational damage can still be a powerful motivation for businesses. For example, in one case where a breach had led to spam emails being sent to a firm's customer database, their main concern was to contact customers as soon as possible to try to limit the reputational impact, even though this diverted a lot of staff away from their main jobs. For some participants reputational damage was especially serious because:

- its effect could linger for much longer than the actual breach, for instance in terms of customers refusing to use the firm again, or regulators investigating or fining the business
- it was more challenging to counteract, as the organisation might not know whether they had reached all the customers or other individuals affected
- in certain circumstances, particularly where the business relied on a small number of key customers, losing just one customer could make an immediate substantial impact on profitability.

"The nature of our business is in being very personal with our customers and speaking to them almost like friends. If someone sent an email to everybody and said we had closed down, for example, five per cent of our database would just remove our email address just because of that."
Small business

"If some of that personal information for one of our large customers got out there, that could be used against us and it could lead to us losing that customer potentially. If we lost one of our top three customers, it wouldn't take the business down but it would put a massive dent in the profit."
Medium business

Some participants also mentioned recent high-profile cyber security breaches appearing in the news that served to reinforce the potential size and depth of reputational damage.

Qualitative case study: how being proactive can help avoid reputational damage

An asset finance company recently found that someone else had used their logos and intellectual property to set up a website with their identity, and then sent emails to staff and clients asking for bank payments to be made. The main impact of this breach was the staff time taken up having to contact clients to explain the situation. Initially they tried to email customers, but one of the unforeseen consequences of the breach was that their company emails had been blocked as spam by many clients. However, the company reported that they did not suffer long-term reputational damage because they managed to mitigate the situation quickly, contacting clients by telephone and alerting them to the breach.

Time taken to recover from breaches

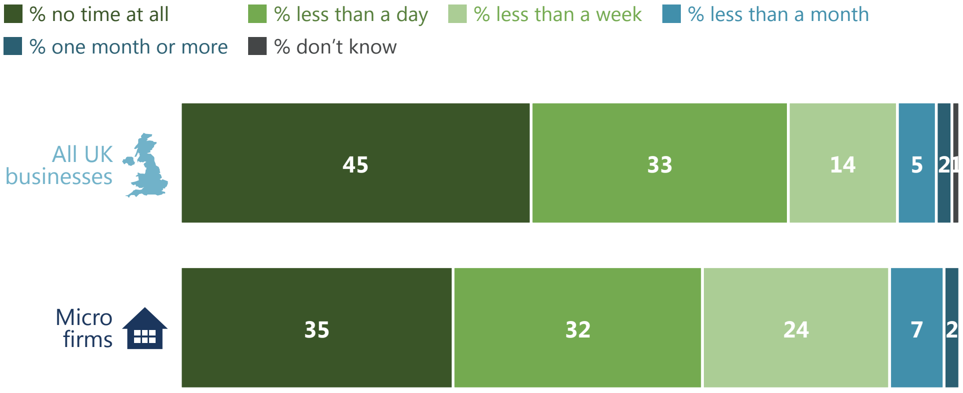
For eight in ten businesses that have experienced breaches (78%), it took less than a day to recover from their most disruptive breach in the last 12 months. As Figure 5.5 shows, over two-fifths (45%) are dealt with immediately.

This reflects the qualitative findings which suggest that, outside of exceptional cases that businesses would generally not experience first-hand, cyber security breaches were generally considered to be minor irritants that were often dealt with automatically by antivirus software or quickly taken care of by an outsourced provider. In other words, due to the nature of most detected breaches being relatively insignificant, some participants did not consider cyber security breaches overall to be a serious threat to their business.

As Figure 5.5 also illustrates, it often takes micro firms slightly longer to recover from a breach, with a quarter (24%, versus 14% overall) saying it took up to a week to recover from their most disruptive breach. This perhaps reflects micro firms' relative lack of infrastructure, specialist staff or protections, such as up-to-date software, as evidenced throughout Chapter 4.

Figure 5.5: Time taken to recover from the most disruptive breach of the last 12 months

Q. How long, if any time at all, did it take to restore business operations back to normal after the (most disruptive) breach or attack was identified?



Bases: 428 that had a breach or attack in the last 12 months; 53 micro firms

In terms of actual manpower, it is large firms that lose the most time on average when dealing with breaches, as shown in Table 5.2. This suggests that the most disruptive breaches faced by businesses in this size band are either more complex, or that larger firms have more sophisticated systems that take longer to repair.

Table 5.2: Average time dealing with the most disruptive breach of last 12 months

	All businesses	Micro/small[33]	Medium	Large
Mean days	2.3	2.2	2.2	4.3
Median days	1	1	1	1
Base	416	107	175	132

5.3 Financial cost of breaches

Assessing costs

It is very uncommon for businesses to have ongoing monitoring of the financial cost of cyber security breaches, with just five per cent of firms saying they do this. Among large businesses this is higher but still unusual, at 13 per cent. Similarly, regular monitoring is more likely than average but still relatively rare among financial or insurance firms (14%).

Even the organisations that rate online services as being core to their business to a large extent do not differ significantly from the average in this respect.

The qualitative findings indicate that businesses face various barriers to accurate financial monitoring, and may therefore underestimate the costs they do and will incur from cyber security breaches.

[33] Micro and small firms have been merged to make this analysis more statistically robust.

- The opportunity costs of breaches were generally considered to be intangible so harder to estimate. Even where they did not regularly monitor costs, participants could retrospectively note the obvious direct costs of breaches, such as money stolen from company credit cards, number of working days lost to disruption and time directly spent dealing with the breach, but they did not typically factor in the opportunity costs of this disruption, such as sales they would have otherwise made.

- Some participants said they did not plan to look at the financial cost of breaches because they felt there was no strong imperative to do so. In some cases this was because senior managers had not asked for any costings. Participants from smaller businesses also felt that because their current spending on cyber security was negligible, they did not think it was worth further investment to monitor the cost of breaches. In another example, one participant felt it was enough for cyber security breaches to be listed as a serious risk on the business's risk register, and that estimating costs would not drive further action.

- Finally, some participants acknowledged that their approach to monitoring costs was not sophisticated, but they could not think of a better way. Some businesses considered costs in terms of broad worst-case scenarios. In one example, the business had a broad rule of thumb directly converting a proportion of lost web traffic during a breach to lost customers and could not see a better way of costing. These businesses were interested in getting more advice on how to effectively monitor costs.

"A standard business day is worth about £25,000 to us. On the days when the website was hacked we'll have seen half as much traffic as we would normally expect, so between those incidents we probably lost £30,000 that wouldn't be recoverable."
Large business

Those who had incurred breaches also attested to how the initial impact could have knock-on effects which were not anticipated, so would not be factored into perceived costs.

- One business that tried to contact clients after someone else had impersonated them online found that many clients' email accounts were now blocking their emails as suspected spam.

- A private school had a ransomware virus that took down their network. This caused unprecedented disruption including the school having to turn contractors away for scheduled work because they could not access the shared drive.

- Another business found themselves blacklisted by Google for three days after their website was hacked, which meant customers could not get onto their site until they had rectified the issue with Google.

"We do frequently check where we appear on Google and one morning we suddenly found that we had a little note underneath the site saying, 'warning, this site's blacklisted,' so we had to learn about how you un-blacklist yourself."
Large business

Overall cost of breaches

The survey asked businesses to estimate the costs they incurred from cyber security breaches, taking into account all the impacts they mentioned resulting from these breaches (as noted in Figure 5.4). As the previous section highlights, it is probable that in some cases businesses have underestimated the costs, and the true values may be slightly higher.

As Table 5.3[34] shows, larger firms tend to incur much more substantial costs from all the cyber security breaches they experience, possibly again reflecting that they may be incurring more complex or challenging breaches, or have more sophisticated systems that are harder to repair. It might also reflect that larger firms tend to more accurately monitor the cost of cyber security breaches in the first place (so are less likely to underestimate these costs).

It is notable that while medium firms have experienced a higher volume of breaches in the last 12 months, their average costs from these breaches tends to be lower. It might be that they are having more frequent but more low-level breaches compared to large firms.[35]

Once again, median estimates are considerably lower than mean estimates. This highlights that most businesses will not experience breaches with substantive financial consequences – but for the minority of firms that do experience these serious breaches, the costs can be extremely high. Given this uncertainty in terms of expected costs, it can be difficult for businesses to fully understand their return on investment in cyber security. This, alongside the likelihood that some breaches go entirely undetected, could be providing a false sense of security to some businesses.

Table 5.3: Average cost of all breaches experienced in last 12 months

	All businesses	Micro/small[36]	Medium	Large
Mean cost	£3,480	£3,100	£1,860	£36,500
Median cost	£200	£200	£180	£1,300
Base	406	107	173	126

Costs associated with the most disruptive breaches

Table 5.4[34] shows cost estimates for the single breaches that caused the most disruption to businesses that experienced breaches (within the last 12 months). The fact that these estimates tend to be fairly close to the overall costs across all breaches (Table 5.3) highlights that individual breaches or attacks can have large financial ramifications for a business. It is worth noting that the most costly single breach captured in this survey is purported to have cost £3 million, and this single event represented the entire estimated cost of cyber

[34] Figures are presented to 3 significant figures or to the nearest whole number.

[35] Once again, it should be noted that while the mean figure differences by size band are large, they are not statistically significant due to large variation within the data. Nevertheless, looking at the broad pattern by size still provides valuable insights.

[36] Micro and small firms have been merged to make this analysis more statistically robust.

security breaches in the last 12 months for the business in question. This case highlights the importance of taking action to prevent and protect against these kinds of attacks.

Table 5.4: Average cost of the most disruptive breach experienced in last 12 months

	All businesses	Micro/small[36]	Medium	Large
Mean cost	£2,620	£2,300	£837	£32,300
Median cost	£100	£100	£48	£323
Base	406	107	172	127

6 Dealing with breaches

This chapter explores how well firms deal with breaches, including identification, response, reporting and adaptation to prevent future breaches.

In the survey, questions on these topics were generally framed in terms of the most disruptive breach a firm had faced in the last 12 months. Sector and regional subgroup analysis has not been undertaken on these questions due to small sample sizes (within businesses that have experienced breaches).

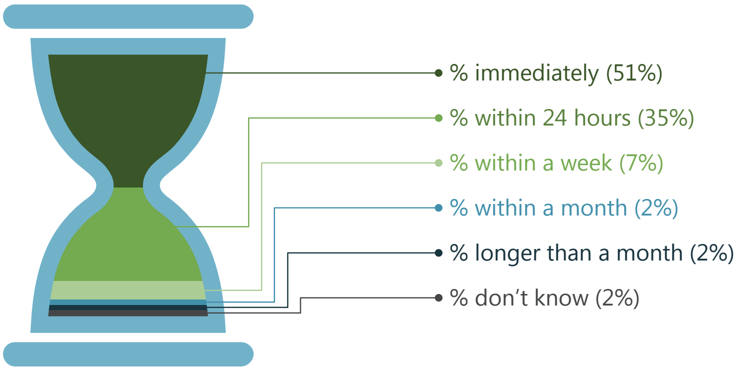
6.1 Identifying and understanding breaches

How and when were breaches identified?

In over four-fifths of cases, even the most disruptive breaches were identified either immediately (51%) or within 24 hours of occurring (35%), as Figure 6.1 indicates.

Figure 6.1: Time taken to identify the most disruptive breach of the last 12 months

Q. How long was it, if any time at all, between this breach or attack occurring and it being identified as a breach?



Base: 428 that had a breach or attack in the last 12 months

When asked unprompted how their most disruptive breach was identified, the top responses from businesses are that it was found by staff or contractors working at the organisation (30% overall, and 50% in larger organisations), picked up by antivirus software (20%) or noticed in terms of disruption to business activities (13%). Discovery by staff or other personnel is much more common than discovery externally, such as through website takedowns (4%), customer reporting (3%) or alerts from external IT providers (3%).

How well do businesses understand their breaches?

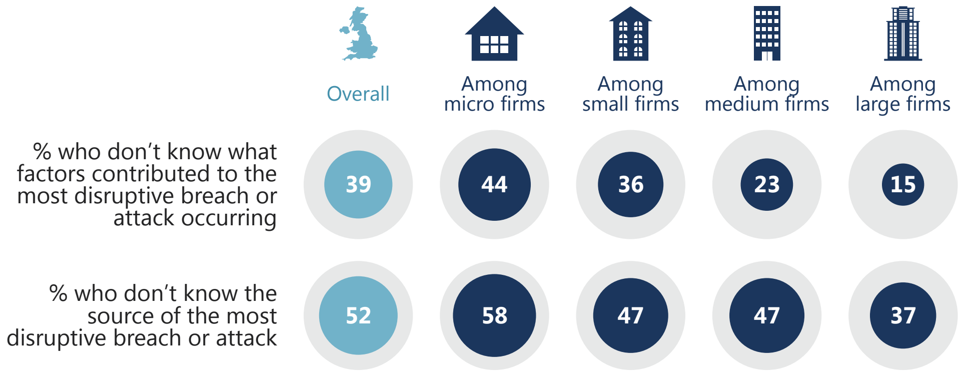
In six in ten cases overall, businesses consider their most disruptive breaches to have been intentional (61%) rather than accidental (26%). The findings for large firms specifically indicate that they may be dealing with more accidental breaches (39% say their most disruptive breach was accidental, versus 29% overall).

Intentional attacks are frequently seen to succeed because of human error. This is the most common single factor that businesses see as having led to their most disruptive breach (in 14% of cases overall, and 28% of cases among large firms). This highlights the importance of awareness and understanding around cyber security across all levels of staff. As aforementioned in this report, businesses can use the Government's free online training courses to help raise awareness among frontline staff, as well as board members.[37]

Email attachments or websites are most commonly identified as the source of the most disruptive breaches (by 28% of organisations overall, and 41% of large organisations). Employees or former employees are seen to be the source of the most disruptive breach in just seven per cent of cases.

It is worth noting that businesses do not always understand the factors and sources behind the breaches they face. Figure 6.2 highlights that around two-fifths of micro and small businesses do not know what led to their most disruptive breach and at least half do not know the source. Even among medium and large firms which tend to have more sophisticated approaches to cyber security, a significant minority say they do not know what factors contributed to their most disruptive breach.

Figure 6.2: Businesses' understanding of the factors and sources behind their most disruptive breaches of the last 12 months



Bases: 428 that had a breach or attack in the last 12 months; 53 micro firms; 58 small firms; 179 medium firms; 138 large firms

6.2 Responding to breaches

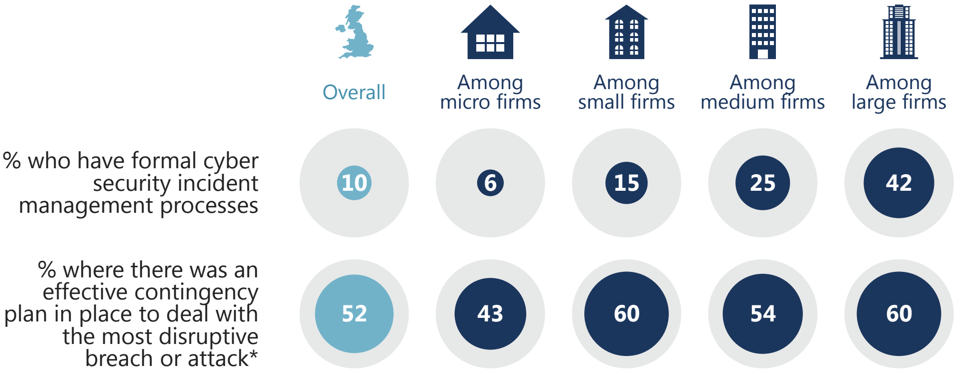
Were there response plans in place?

As can be seen in Figure 6.3, the likelihood of there being plans in place to deal with breaches varies by the size of the business. Half of all firms (52%) and six in ten larger firms (60%) who experienced breaches in the last 12 months say they had effective contingency plans to deal with their most disruptive breach.

Even among large businesses however, most businesses do not have formalised incident management processes. These processes seem to be more common in financial or insurance firms (29%, versus 10% overall) and information, communications or utility firms (20%).

[37] See https://www.gov.uk/government/collections/cyber-security-training-for-business.

Figure 6.3: Whether businesses have incident management processes and contingency plans



Bases: 1,008 UK businesses (*428 that had a breach or attack in the last 12 months); 278 micro firms (*53); 174 small firms (*58); 349 medium firms (*179); 203 large firms (*138)

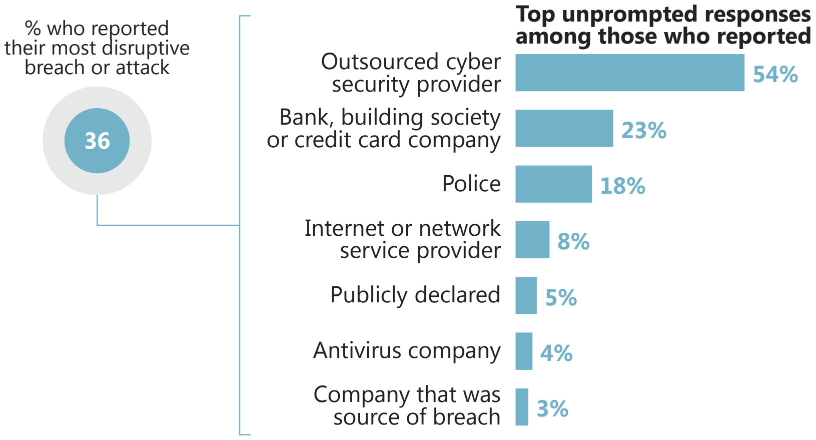
Reporting breaches

External reporting is very limited, as Figure 6.4 illustrates. Just over a third (36%) reported their most disruptive breach, and most commonly this was reported only to an outsourced cyber security provider (where the reporting might be to enable them to make repairs). When excluding for those reporting solely to outsourced providers, only a fifth (21%) of the most disruptive breaches were externally reported.

Outside of the police, public sector agencies do not tend to be common reporting locations for businesses that have experienced breaches (accounting for four per cent of all reporting). While these are not among the top unprompted responses, the public sector agencies mentioned in a handful of instances include regulators such as the Financial Conduct Authority, Prudential Regulation Authority or Information Commissioner's Office and Action Fraud (the UK's national fraud and cyber crime reporting centre).

Figure 6.4: Reporting of the most disruptive breaches of the last 12 months

Q. Who was this (most disruptive) breach or attack reported to?



Bases: 428 that had a breach or attack in the last 12 months; 146 that reported the attack

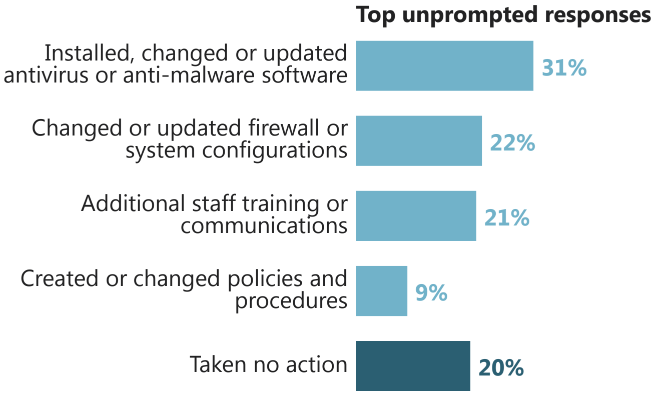
Of course, the relatively sporadic mentions of public or policing bodies could reflect the fact that businesses may not see their breach as criminal. The qualitative work suggests that where businesses do not lose assets or customer data, they may not necessarily see the point of reporting their breach. This suggests that if reporting is to become more frequent, businesses may need to better understand when and why they should be reporting. For example, reporting breaches to Action Fraud can help to aggregate similar patterns of activity, and allow policing bodies to investigate whether there is any criminal intent and take appropriate steps.

Preventing future breaches

The most common actions taken following breaches are around bringing in or updating antivirus or anti-malware software, and firewall configurations, or raising staff awareness via training or communications. Relatively few have created or updated cyber security policies in response to their most disruptive breach, and a fifth (20%) have taken no action at all. The top unprompted mentions are shown in Figure 6.5.

Figure 6.5: Most common actions following the most disruptive breach of the last 12 months

Q. What, if anything, have you done since this (most disruptive) breach or attack to prevent or protect your organisation from further breaches like this?



Base: 428 that had a breach or attack in the last 12 months

The qualitative research highlights how having a cyber security breach that is noticed by customers or leads to the loss of data can often be a tipping point for an organisation. Several examples from interviews involved businesses spending substantial amounts on cyber security following a breach, for example to take out cyber security insurance or, in one case, to replace all the organisation's existing servers with Remote Desktop Services following a laptop theft.

Qualitative case study: how a breach can prompt a full review of cyber security

A small greeting card publisher said that they treat their electronic artwork as their most valuable asset, and back up these electronic files to a cloud server. Two years ago they had a ransomware virus on one of their email servers and were forced to wipe the server clean. While the attack did not cause significant damage financially or in terms of reputation, it highlighted to them how any business can be attacked and the potential threat to their stored artwork. They have since ensured that all servers have up-to-date antivirus software and have a more centralised system where the IT Manager gets alerted by email if there are any server security issues.

7 Conclusions

The Cyber Security Breaches Survey shows definitively that cyber security is an issue affecting virtually all UK businesses. The overwhelming majority of businesses operate online in some form and many consider themselves to be online businesses as much as offline ones. The widespread use of cloud computing and the fact that many employees use personal devices for work creates additional risks for businesses to consider.

Most businesses say they treat cyber security as a high priority. Nevertheless, not all of these businesses are investing or taking significant action to protect against cyber security risks. In addition, while most senior managers may take cyber security seriously, they can often be divorced from the actions taken to protect their organisations and can lack the appropriate knowledge or expertise to engage more with the topic.

Moreover, the overall findings mask substantial variation by size and sector. Across a range of indicators, there are lower than average levels of engagement with cyber security within construction or manufacturing firms, entertainment, service or membership organisations, and the food or hospitality sectors, as well as among micro and small firms generally.

At the same time, the findings help to pinpoint the major challenges, and potential solutions, around getting businesses of all sizes and from all sectors to better protect themselves against breaches:

- While many businesses are leading the way with formalised approaches and technical controls, most still do not have cyber security policies, and significant minorities do not implement basic security controls or user-access controls on their devices. These are basic steps that most businesses can still take to better identify and manage their cyber security risks.

- Micro and small businesses as well as those in less engaged sectors tend to have less infrastructure and expertise to manage their cyber security. These businesses may particularly benefit from being more aware of the existing range of Government communications and signposting to resources on cyber security, such as the small business guidance, 10 Steps guidance and Cyber Essentials.

- For these smaller and less engaged businesses, cyber security can also be reframed so that it is not just considered as an IT problem that is beyond their scope or understanding. Approaching cyber security as a compliance or business performance issue may help these businesses to see the value of investing in it. More broadly, building up a staff culture that emphasises confidentiality and good data management could also lead small businesses into an instinctively good approach to cyber security.

- There are also specific areas that medium and large businesses should review to ensure they are taking a comprehensive approach to cyber security. While these businesses are typically more advanced in terms of their approaches, many still have gaps when it comes to implementing data encryption rules, offering staff training, and having formal incident management processes. Many larger businesses could also make use of their market power to raise minimum standards among their smaller suppliers.

- Whether a business chooses to invest in cyber security often rests on key individuals and the support they receive within the business. Currently most businesses do not have board members with any specific responsibilities around cyber security. Bringing in board-level oversight and expertise might be an important precursor to more businesses taking action.

- Across all businesses, the costs of cyber security breaches may be underestimated for a variety of reasons, and many businesses may assume the costs are negligible, despite potentially substantial costs resulting from a single disruptive breach. In this environment, a kneejerk response can be to deprioritise cyber security. Highlighting cautionary tales, real-life consequences and even worst-case scenarios could help to maintain senior managers' engagement in these cases.

- Currently most cyber security breaches are not reported at all. Even when they are reported, there is no specific public sector agency seen to deal with this issue. This may change when the National Cyber Security Centre comes into being in 2016, but even then businesses may need a better understanding of when, where and why they should be reporting breaches before this becomes the norm.

Of course, this is only the first in a proposed series of annual surveys. Future surveys will be able to examine progress over time on each of these areas and will continue to inform businesses on how they can best deal with the evolving cyber security threat.

Guide to statistical reliability

It should be remembered that final data from the survey are based on a weighted sample, rather than the entire UK business population. Percentage results are therefore subject to margins of error, which vary with the size of the sample and the percentage figure concerned.

For example, for a question where 50% of the 1,008 businesses sampled in the survey give a particular answer, the chances are 95 in 100 that this result would not vary more or less than 4.7 percentage points from the true figure – the figure that would have been obtained had the entire population responded to the survey. The margins of error that are assumed to apply in this report are given in the following table.[38]

Margins of error applicable to percentages at or near these levels

	10% or 90% ± (% points)	30% or 70% ± (% points)	50% ± (% points)
1,008 UK businesses	2.8	4.3	4.7
282 micro firms (2 to 9 employees)	3.7	5.6	6.1
174 small firms (10 to 49 employees)	4.7	7.1	7.8
349 medium firms (50 to 249 employees)	3.3	5.0	5.5
203 large firms (250 employees or more)	4.4	6.7	7.3

There are also margins of error when looking at subgroup differences. A difference must be of at least a certain size to be statistically significant. The following table is a guide to these margins of error.

Differences required from overall result for significance at or near these percentage levels

	10% or 90% ± (% points)	30% or 70% ± (% points)	50% ± (% points)
282 micro firms	3.8	6.3	7.2
174 small firms	4.3	7.3	8.5
349 medium firms	3.7	6.0	6.8
203 large firms	4.1	7.1	8.1

[38] In calculating these margins of error, the design effect of the weighting has been taken into account.

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos-mori.com
http://twitter.com/IpsosMORI

About Ipsos MORI's Social Research Institute
The Social Research Institute works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. This, combined with our methodological and communications expertise, helps ensure that our research makes a difference for decision makers and communities.