October **2017**

Ipsos Public Affairs

The cybercrime threat to corporate reputation

Carl Phillips | Becky Writer-Davies | Mark McGeoghegan

GAME CHANGERS

Anyone who regularly reads the news would be forgiven for thinking that cybercrime was endemic across the world at the moment. Scarcely a week goes by without a new story, and while many of them are newsworthy for only a short time, as these attacks increase in number so will the frequency that they become genuine headline news.

Between May and July this year, the names, social security numbers, and in some cases credit card numbers of over 140 million Americans (almost half of the American population) were stolen from the US credit firm Equifax. In May, a global cyber-attack locked up over 200,000 computers using a ransomware virus, demanding payment in the cryptocurrency Bitcoin in exchange for not erasing data. Notable among the victims was the NHS. September gave us the revelation that Deloitte, a major player in cybersecurity consultancy, had its email server hacked due to the lack of two-step verification.

A choice selection of stories from the last couple of years would include the details of 500 million Yahoo users stolen, 165 million accounts hacked at LinkedIn and similar numbers hacked at Adobe. The list of affected companies and organisations is long – Tesco Bank, the World Anti-Doping Agency, eBay, Target, JP Morgan, Sony, Home Depot, Anthem, Premera Blue Cross – and grows by the month.

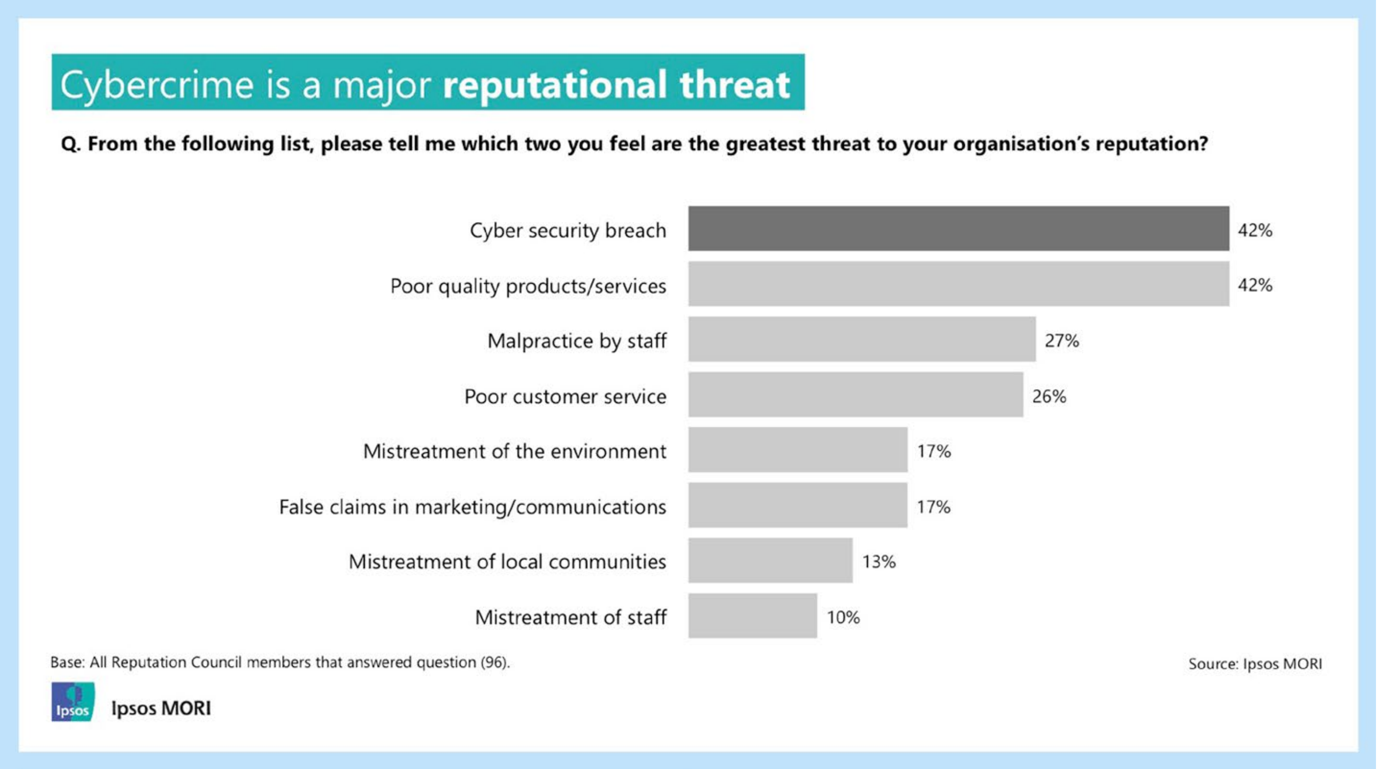
Furthermore, this is without addressing the highest profile of them all, the alleged Russian hack of the Democrats in the US which, depending on your point of view, had major ramifications for the Presidential election. This was then followed up by similar events in the French Presidential election, although the impact was less.

While the short-term impacts of these events are usually identifiable, be they a denial of service, the theft of data, the loss of assets or just simple embarrassment, the longer term impact is harder to quantify. For many people, both in business and in politics, the true threat of cybercrime is one’s reputation. Companies fear that the opinions of customers will change as a result of a hack or data breach. Customers who allow companies to collect their personal information, be it their addresses, billing information or user history, have an expectation that this information will be stored securely and used responsibly. It is therefore expected that a company, with all of the resources at its disposal, should invest in defences that prevent hackers from accessing that information. Failure to do so reflects badly on the company, and if customers are inconvenienced as a result there is always the risk that they will take their custom elsewhere.

At the heart of this is trust: customers trust that companies, and indeed public sector organisations, will keep their information safe and provide the service they promise. Cybercrime is therefore a very real threat to the reputation of a company, and this threat has not gone unnoticed by the worlds of business and politics. Whether the right level of action has been taken to combat the threat however is another question.

> **“**
>
> **If they can’t secure your data why would you trust them with anything else?**
>
> - Conservative MP

Research from Ipsos MORI’s Reputation Council, a panel of senior corporate communicators and public affairs directors from across the globe, shows that they see a cyber security breach as the greatest threat to their company’s corporate reputation.



Cybercrime is a major **reputational threat**

Q. From the following list, please tell me which two you feel are the greatest threat to your organisation's reputation?

Base: All Reputation Council members that answered question (96).

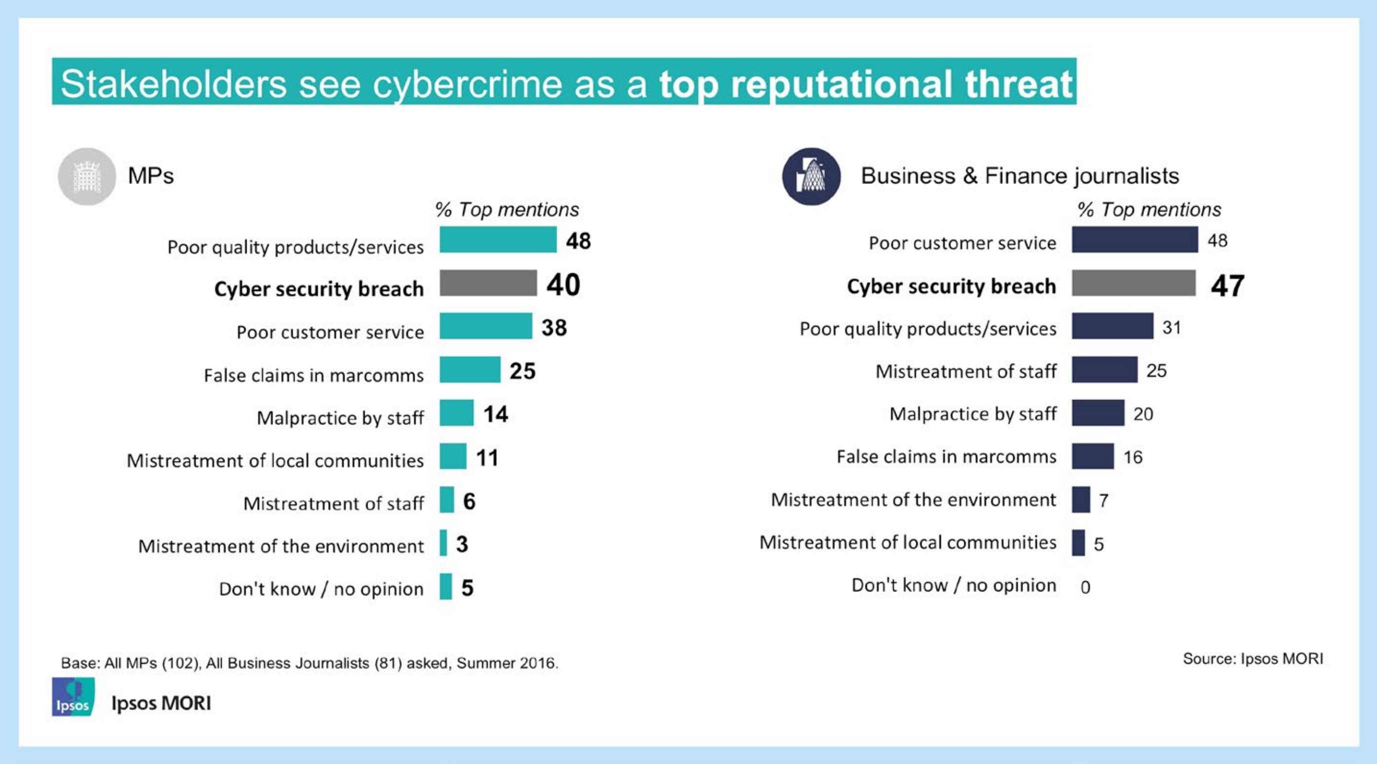
Source: Ipsos MORI

Ipsos MORI

Council members recognise cybercrime as one of the greatest risks to an organisation's reputation: two-fifths (42%) cite it as one of their main concerns, putting it on par with risks such as product quality and staff malpractice, that are decades, if not centuries, old.

Concern is not confined to corporate communications personnel alone; a similar sentiment is echoed by both parliamentarians and business journalists. While both say that product or service issues are a company's primary reputational threat, cybercrime comes a close second.

> **"It keeps me up at night. Whichever industry you are in you are absolutely not untouched by cyber criminals**
>
> - Reputation Council member



Base: All MPs (102), All Business Journalists (81) asked, Summer 2016.

Source: Ipsos MORI

Scale of the threat

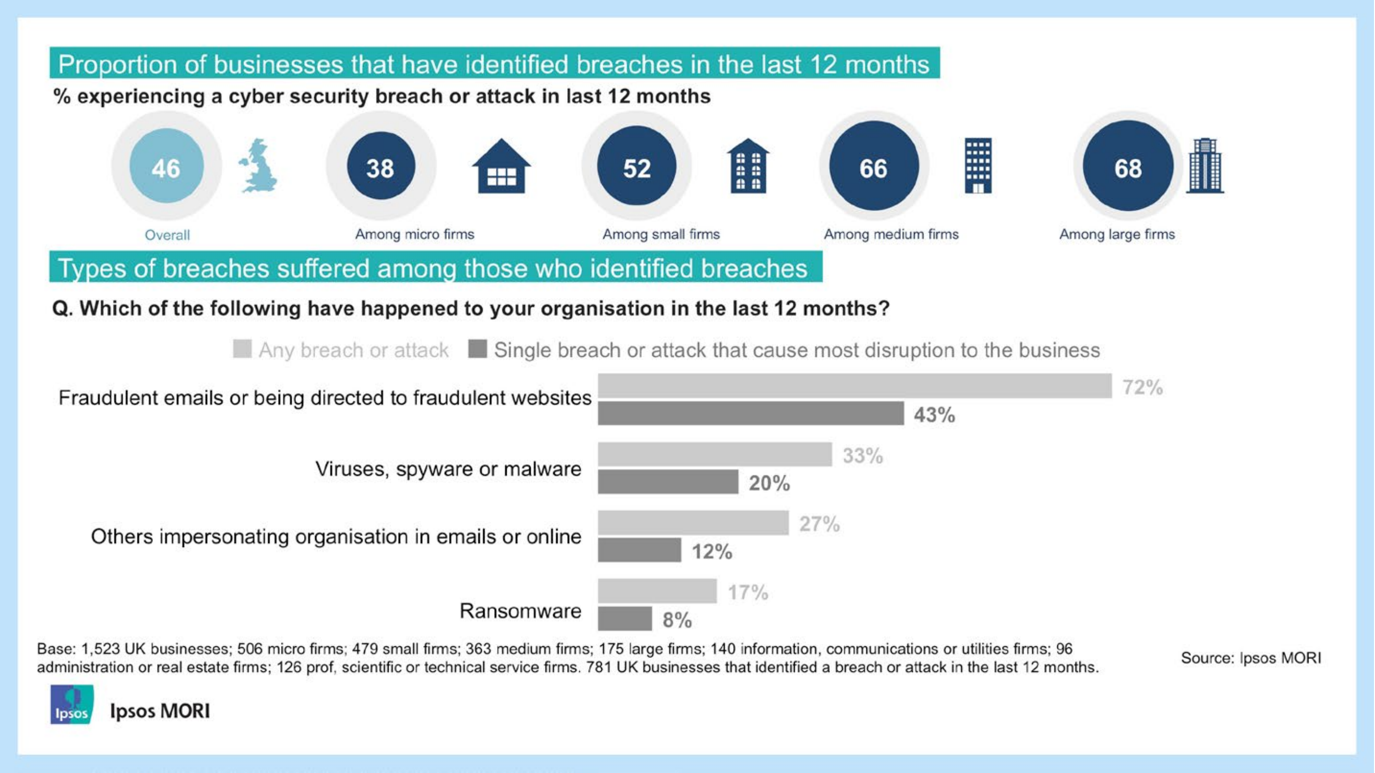
These concerns are not misplaced. Given the pace of change in the IT infrastructure that underpins many modern businesses, including everything from cloud computing through to mobile and remote working, and the increase in automation in industry, businesses are dependent on integrated IT infrastructure to a level never before seen. As this trend continues, the interconnectivity and the associated weaknesses of those networks will be targeted.

More and more UK businesses rely on online services. Indeed, three in five consider them as core to their business offer. Almost all UK businesses (99%) now employ online services in some way; 91% provide employees with a company email address, 85% have a website, 61% store their customers' personal data electronically and 59% have a social media account.

The use of cloud services is also increasing: 6 in 10 (59%) now use some form of externally-hosted web service, with three in five (60%) storing commercially confidential information on the cloud and over half (55%) storing personal data relating to customers, staff or suppliers.

Just as businesses are expanding the amount they say and do online, the threat posed by cybercrime is also expanding. In the recent Ipsos MORI Cyber Security Breaches Survey – commissioned by the Department for Culture, Media and Sport as part of the National Cyber Security Strategy – almost half (46%) of businesses surveyed had identified a breach or attack in the last 12 months. Among businesses holding electronic personal data on their customers this rose to just over half (51%). Most common forms of attack included staff receiving fraudulent emails (72%), the use of viruses, spyware and malware (33%), people impersonating the organisation in emails or online (27%) and ransomware (17%).

> “The government needs to make sure it is working closely with big businesses to make sure they have robust systems in place, because it is a matter of national reputation as much as individual companies’ reputations
>
> - Conservative MP



Proportion of businesses that have identified breaches in the last 12 months

% experiencing a cyber security breach or attack in last 12 months

Types of breaches suffered among those who identified breaches

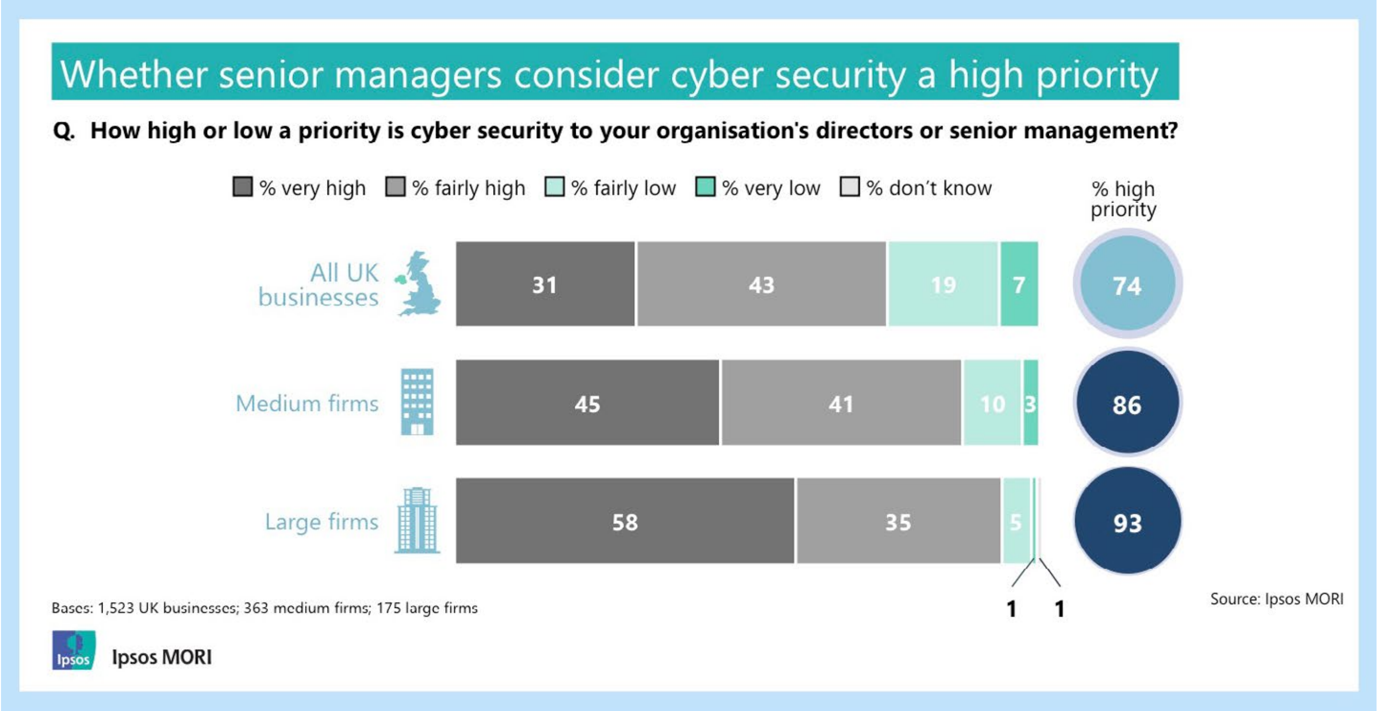
Q. Which of the following have happened to your organisation in the last 12 months?

Base: 1,523 UK businesses; 506 micro firms; 479 small firms; 363 medium firms; 175 large firms; 140 information, communications or utilities firms; 96 administration or real estate firms; 126 prof, scientific or technical service firms. 781 UK businesses that identified a breach or attack in the last 12 months.

Source: Ipsos MORI

Ipsos MORI

Among those experiencing an attack, four in ten (41%) saw a material outcome, most commonly the temporary loss of access to files or network (23%). Just 6% reported having money stolen, and 4% having personal data destroyed, altered or taken. While these figures do serve to remind us that the vast majority of cybercrime is, at best, a nuisance, the rising frequency will mean that incidents that have a real chance of causing significant damage or disruption, and potentially becoming newsworthy, will become more common.



Whether senior managers consider cyber security a high priority

Q. How high or low a priority is cyber security to your organisation's directors or senior management?

Bases: 1,523 UK businesses; 363 medium firms; 175 large firms

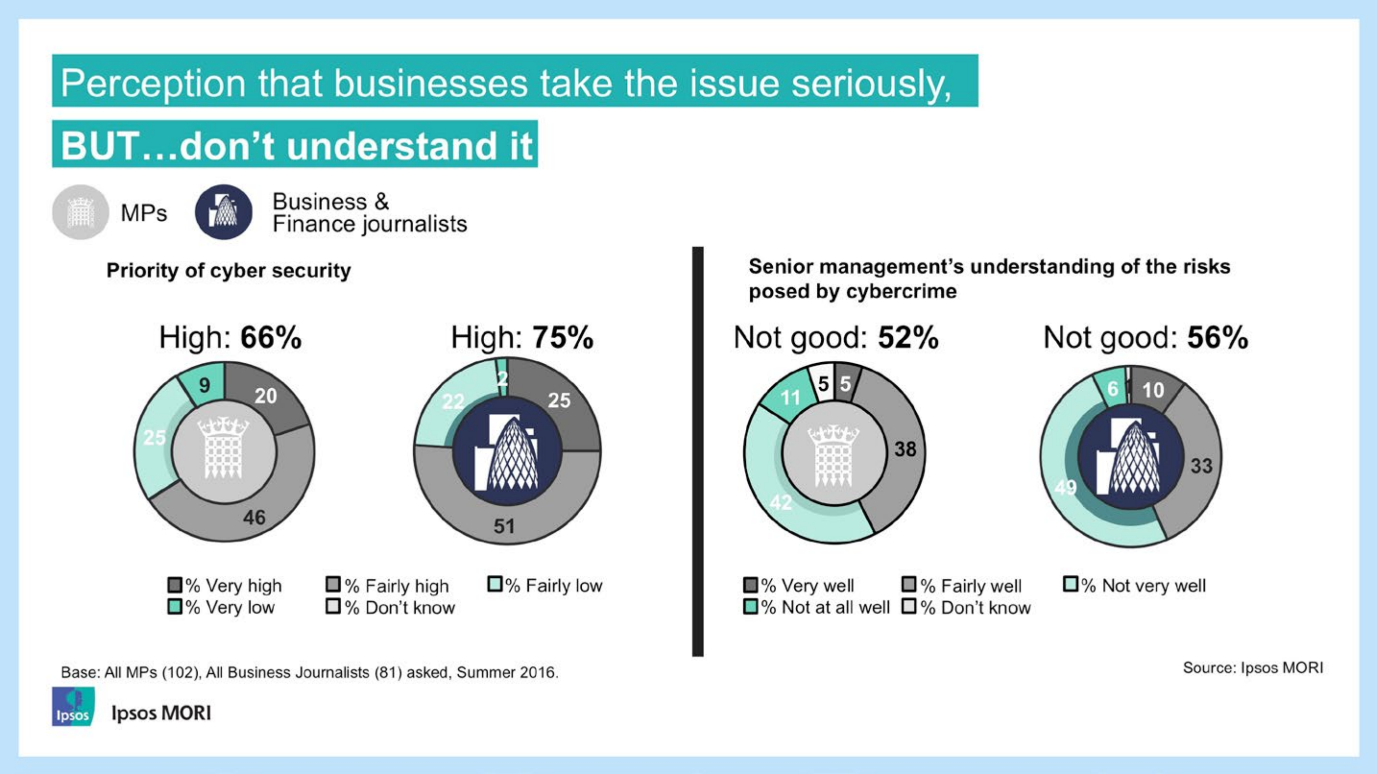
Source: Ipsos MORI

Ipsos MORI

While the majority (81%) of businesses experiencing attacks said they were able to deal with the consequences of these attacks within 24 hours, implying only a short-term impact on business functionality, the long-term impact on their relationship with customers and stakeholders for many is unknown (just 6% of firms say they attempt to estimate how much a cyber security breach or attack cost their organisation financially, and none admit to tracking its impact on customer sentiment).

And as the prevalence of cybercrime increases, the importance of cyber security to consumers has risen. Two-thirds (67%) of consumers now say they are concerned that cybercrime could affect their bank account or other financial holdings, while a little under half (47%) say they trust most large companies to keep their data secure. There is the possibility that these concerns could materialise in a boycott after an attack; over half (56%) of consumers say that if a financial services company was a victim of cybercrime, it would make them less likely to use that company in the future.

> **“It would be a catastrophe for our reputation if the information should leak. It would have a long-term effect on our reputation**
>
> - Reputation Council member



Perception that businesses take the issue seriously,

BUT…don't understand it

MPs Business & Finance journalists

Priority of cyber security

High: **66%** High: **75%**

■ % Very high ▨ % Fairly high □ % Fairly low
🟩 % Very low □ % Don't know

Senior management's understanding of the risks posed by cybercrime

Not good: **52%** Not good: **56%**

■ % Very well ▨ % Fairly well □ % Not very well
🟩 % Not at all well □ % Don't know

Base: All MPs (102), All Business Journalists (81) asked, Summer 2016.

Source: Ipsos MORI

Ipsos MORI

Tackling cybercrime

Naturally, this is concerning to UK businesses and they do not take the threat posed by cybercrime lightly. Almost three-quarters (74%) say that cyber security is a high priority for their senior management, with three in ten (31%) saying that it is a very high priority. The key point here though is not the number who think cybersecurity is a high priority, it's the minority who don't.

This is echoed by stakeholders – while two-thirds (66%) of MPs and three in four (75%) business journalists believe that cyber security is a high priority for senior management, the fact there is any doubt at all is worrying.

Furthermore, stakeholders are not convinced that the directors and senior management of major companies really understand the threat or how to combat it. More than half of MPs and business journalists believe that directors and senior management do not understand the risks posed by cybercrime very well, if at all. Awareness of the risks posed by cybercrime is high amongst both senior management and stakeholders, but despite the high priority being accorded to the cybercrime threat there is little faith that British businesses are capable of tackling it.

This core concern appears to be grounded in reality. Just under one in three (32%) UK businesses have spoken with external experts about cyber security threats – with less than one in twenty (4%) having sought out Government or other public sector sources of guidance – and only one-third (33%) have a formal cyber security policy. Accordingly, awareness among businesses of basic cyber security standards is also low, with only one in five (21%) being aware of the International Standards Organisation's standards for information security management, and even lower awareness of UK government initiatives.

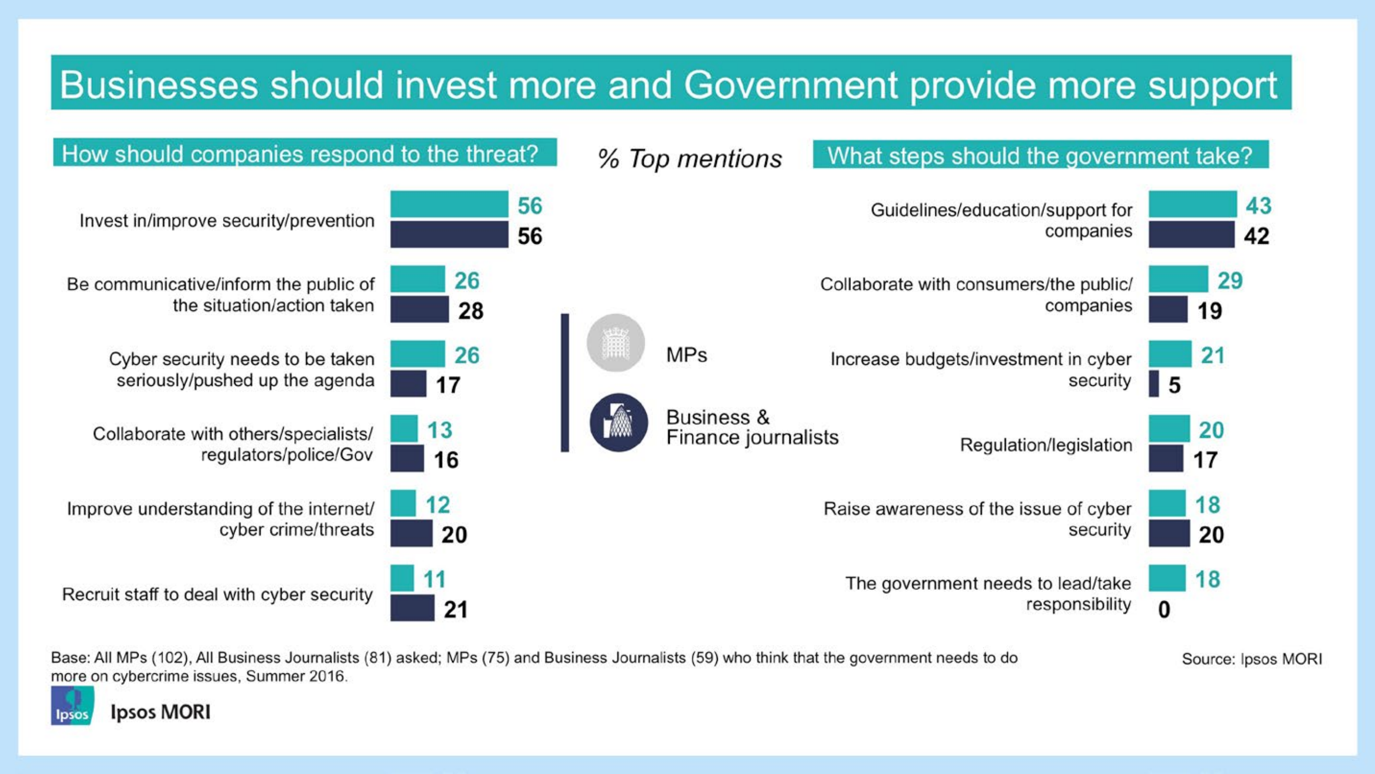
Considering what they believe businesses ought to do, stakeholders view investment in cyber security and the prevention of cybercrime as the key actions UK businesses should take to address the reputational risks of cybercrime, with more than half of MPs and business journalists mentioning some kind of investment in security as essential.

When breaches do occur, both groups tend to believe that businesses should be more communicative: quicker to inform the public when they suffer a breach, and clearer about the actions they take to tackle breaches and improve security.

Investment is taking place, but the depth of it is questionable. While two-thirds (67%) of UK businesses spent money on cyber security last year, this amount ranged from a median spend of just £200 among micro and small businesses to £21,200 among large businesses. Only three in ten (30%) businesses have invested in staff training, under two in five (37%) have established a segregated wireless network, and the same proportion have implemented rules around the encryption of confidential data. Businesses perform even worse on transparency, with just over a quarter (26%) reporting their most disruptive breach in the 12 months to January 2017.

What this demonstrates is that while most UK businesses are spending on improving their cyber security, they are nevertheless falling short of stakeholders' expectations. Low levels of investment in cyber security, coupled with the fact that the majority of British businesses have not invested in the key components of a good cyber security strategy, suggests that stakeholders are right to be worried that the senior management of Britain's businesses lack the knowledge and inclination to protect their organisations and customers from cybercrime, or to respond effectively or transparently to breaches when they occur.

> “
> **They need to show they are taking it deadly seriously, they need to have someone who is trusted and reliable, who will be the face of the business, who will assume responsibility for it**
>
> - Business journalist



Base: All MPs (102), All Business Journalists (81) asked; MPs (75) and Business Journalists (59) who think that the government needs to do more on cybercrime issues, Summer 2016.

Source: Ipsos MORI

Stakeholders believe that as the threat posed by cybercrime grows, the UK Government needs to do more to tackle the issue. Three in four MPs (74%) and a similar proportion of business journalists (73%) say that the Government needs to take more action.

As a response, in the past year the Government has stepped up its efforts to protect British institutions, businesses, and individuals. In October 2016, the National Cyber Security Centre (NCSC) was established to co-ordinate the efforts of Government agencies to prevent cybercrime. The NCSC has established and grown the Cyber Security Information Sharing Partnership (CiSP), a joint venture with British industry to produce and distribute threat reports, advice, and guidance for businesses. The Ipsos MORI Cyber Security Breaches Survey found that, when the NCSC was established, only just over one in ten (13%) businesses had heard of '10 Steps to Cyber Security', and under one in ten (8%) were aware of Cyber Essentials, two of the Government's flagship schemes to help companies step up their cyber security. Since then, according to the NCSC's 2017 Annual Review, organisational membership of CiSP has grown by 43%, yet still fewer than 8,000 British organisations are members. The NCSC still has a mountain to climb in trying to reach greater numbers of British businesses and organisations.

The Government is also putting a lot of store in the upcoming General Data Protection Regulation that will come into force in May 2018. Alongside many of the features of this bill – regarded internationally as an exemplar of government leadership on the issue – is the reiteration of the responsibility of anyone holding personal information on users to keep it safe, and the penalties for failure have been increased. The Government believes that sanctions, such as a fine of up to 4% of a company's annual worldwide turnover, will be a sufficient threat to convince all companies to start regarding cybersecurity as a priority issue.

From a corporate reputation standpoint, the GDPR legislation also makes clear that data controllers are under obligation to report breaches to the supervisory authorities without delay. Recent years have shown a trend for companies to sit on the news for as long as possible, almost certainly to control the media fallout that might ensue. The Cyber Security Breaches Survey shows that only one in four (26%) businesses which identified a cybersecurity breach in 2016 reported it to anyone external to the company except their cybersecurity provider; of those that did report their breach, only one fifth (19%) did so to the supervisory authorities. This is going to change, and the best way to prevent negative media stories is to stop data breaches in the first place.

UK businesses have woken up to the significant reputational threat posed by cybercrime. Improving cyber security is moving up the list of priorities for senior management, and the majority of Reputation Council members are taking substantial measures to respond to the threat. However, most businesses are investing relatively little in improving their cyber security, and most lack the foundations of an effective cyber security strategy.

This is reflected in the views of stakeholders, who have little faith in the ability of Britain's businesses to tackle the threat of cybercrime and protect their companies and customers. Cyber breaches and vulnerability to cybercrime erode trust in UK businesses and undermine individual and collective reputations. Both businesses and Government can and must do more to combat this threat and build trust in their ability to do so.

> **“**
>
> **It is something that can affect a company overnight. Poor service, poor products or false claims can have an effect over a period of time. If you have a cyber security breach, your reputation can be in tatters the next day**
>
> - Reputation Council member

Technical note

MPs Survey

Ipsos MORI interviewed a representative sample of Members of Parliament between 9th June and 26th July 2016. A total of 102 MPs were interviewed, including 50 Conservative MPs, 40 Labour MPs, 7 SNP MPs and 5 other MPs. A mix of both front and back bench MPs were interviewed. For more information, see our MPs Surveys page.

Business and Financial Journalists Survey

Ipsos MORI interviewed a sample of Business and Finance journalists between 1st June and 5th July 2016. A total of 81 journalists were interviewed, including 44 writing for National publications, 24 writing for Regionals, and 13 from Online/Broadcast/Wire media. For more information, see our Business and Finance Journalists Survey page.

Ipsos MORI Reputation Council

Established in2009, the Reputation Council brings together senior communicators from some of the most respected corporations in the world. In 2016, 109 interviews were conducted with Reputation Council members between April and August 2016.

Ipsos MORI Cyber Security Breaches Survey

The Cyber Security Breaches Survey is an Official Statistic and has been produced to the standards set out in the Code of Practice for Official Statistics.

Ipsos MORI surveyed 1,523 UK businesses (including 171 large businesses employing 250 or more staff) by telephone from 24 October 2016 to 11 January 2017. Sole traders and public sector organisations were outside the scope of the survey, so were excluded. In addition, businesses with no IT capacity or online presence were deemed ineligible, which meant that a small number of specific sectors (agriculture, forestry, fishing, mining and quarrying) were excluded. The data is weighted to be representative of all UK businesses (who were in scope). A total of 30 in-depth interviews were undertaken in January and February 2017 to follow up businesses that participated in the survey.

Ipsos Public Affairs

October **2017**

Carl Phillips, Director, Ipsos Global Reputation Centre

Becky Writer-Davies, Research Manager, Ipsos Global Reputation Centre

Mark McGeoghegan, Research Executive, Ipsos Global Reputation Centre

Ipsos Public Affairs works closely with government and international organisations, local public services and the not-for-profit sector. Research staff focus on public service and policy issues. We provide clients with information that helps them understand how they can build efficient and effective policies, programs, communications, strategies and marketing Initiatives. This, combined with our methodological and communications expertise, ensures that our researchmakes a difference for decision makers and communities worldwide.

This *Ipsos Views* paper is produced by the **Ipsos Knowledge Centre.**

www.ipsos.com
@_Ipsos
IKC@ipsos.com

<< Game Changers >> is the **Ipsos** signature.

At **Ipsos** we are passionately curious about people, markets, brands and society. We make our changing world easier and faster to navigate and inspire clients to make smarter decisions. We deliver with security, simplicity, speed and substance. We are Game Changers.

GAME CHANGERS Ipsos