Department for Culture Media & Sport

Ipsos MORI Social Research Institute

University of Portsmouth

April 2017

Cyber security breaches survey 2017

Summary report

Dr Rebecca Klahr, Jayesh Navin Shah, Paul Sheriffs, Tom Rossington and Gemma Pestell
Ipsos MORI Social Research Institute

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

● GENERAL BUSINESS FINDINGS ●

EXPERIENCE OF BREACHES

46% of UK businesses overall identified cyber security breaches or attacks in the last 12 months

45% among micro/small businesses

66% among medium/large businesses

41% among businesses who say online services are not at all core to their business

AMONG THE 46% WHO IDENTIFIED A BREACH OR ATTACK

- **23%** Had a temporary loss of files
- **20%** Had software or systems corrupted
- **10%** Had a permanent loss or change of files or personal data
- **9%** Lost access to third-party systems they rely on
- **9%** Had their website slowed or taken down
- **6%** Had money, assets or intellectual property stolen

PRIORITISING CYBER SECURITY

74% of UK businesses where directors or senior management say cyber security is a high priority

67% of UK businesses overall spend money on cyber security

Among the 67%, the top (unprompted) reasons for spending in this area were:

- To protect customer data **51%**
- To protect trade secrets/assets **28%**
- To prevent fraud **17%**
- To ensure business continuity **14%**
- To protect their reputation **10%**

- Have firewalls with appropriate configurations **89%**
- Restrict IT admin and access rights to specific users **79%**
- Have formal policies covering cyber security risks **33%**
- Have had staff receive or attend cyber security training or seminars **20%**
- Have a cyber security incident management plan **11%**

Bases for graphics on this page: 1,523 UK businesses (excluding agriculture, forestry and fishing businesses, and mining and quarrying businesses); 597 who say online services are not at all core to their business; 781 who identified a breach or attack in the last 12 months; 930 who spend money on cyber security.

● MICRO/SMALL BUSINESS FINDINGS ●

EXPERIENCE OF BREACHES

45% of micro/small businesses identified cyber security breaches or attacks in the last 12 months

£1,380 Average (mean) cost of all breaches identified in the last 12 months

2 Median number of breaches experienced in the last 12 months

19% who had been breached took a day or more to recover from their most disruptive breach

AMONG THE 45% WHO IDENTIFIED A BREACH OR ATTACK

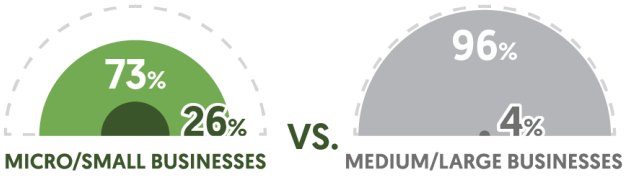
- **37%** Needed new measures to prevent or protect against future breaches
- **33%** Used additional staff time to deal with breaches
- **23%** Said that breaches stopped staff carrying out day-to-day work
- **19%** Said that breaches incurred further recovery or repair costs

TAKING PREVENTATIVE ACTION

57% of micro/small businesses have carried out any health checks, risk assessments or audits to identify cyber security risks

Businesses that have any cyber security governance or risk management measures in place ('don't know' responses not shown)

● HAVE MEASURES IN PLACE ● HAVE NONE



39% of micro/small businesses with no governance or risk management measures think they are too small or insignificant for cyber security

Bases for graphics on this page: 985 micro/small UK businesses with 2 to 49 employees; 427 micro/small businesses who identified a breach or attack in the last 12 months; 206 micro/small businesses who have none of the governance or risk management arrangements listed in the survey (board members with cyber security responsibilities, outsourced cyber security providers, formal cyber security policies, business continuity plans or staff assigned to information security or governance); 538 medium/large UK businesses.

● MEDIUM BUSINESSES ● LARGE BUSINESSES

EXPERIENCE OF BREACHES

66%
68%
of medium/large businesses identified cyber security breaches or attacks in the last 12 months

4 | 8 Median number of breaches experienced in the last 12 months

£3,070 | £19,600
Average (mean) cost of all breaches identified in the last 12 months

AMONG THE 66%/68% WHO IDENTIFIED A BREACH OR ATTACK

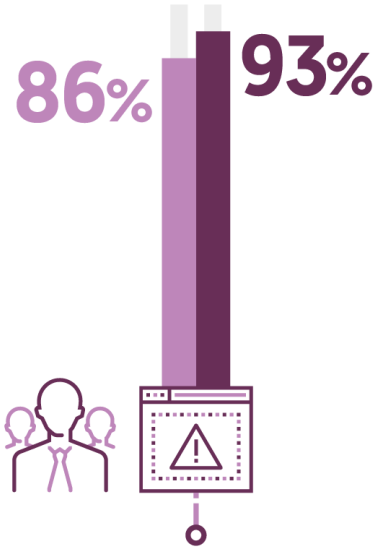
43%
58%
Needed new measures to prevent or protect against future breaches

46%
40%
Used additional staff time to deal with breaches

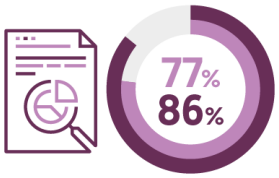
36%
37%
Said that breaches stopped staff carrying out day to day work

18%
22%
Said that breaches incurred further recovery or repair costs

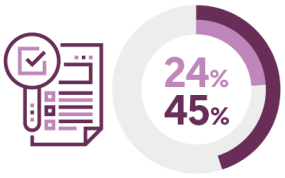
PRIORITISING CYBER SECURITY AND SUPPLIER STANDARDS



86%
93%
of medium/large businesses where directors or senior management say cyber security is a high priority

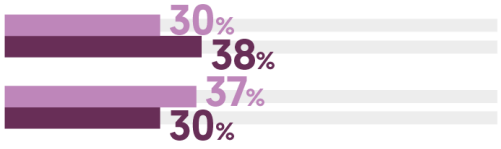


77%
86%
Have carried out any health checks, risk assessments or audits to identify cyber security risks



24%
45%
Have a formal cyber security incident management process

Agree/disagree that the cyber security of their suppliers is "probably not as good as ours"



Require their suppliers to adhere to any cyber security standards or good practice guides

Bases for graphics on this page: 363 medium UK businesses with 50 to 249 employees; 175 large UK businesses with 250 or more employees; 234 medium/120 large businesses who identified a breach or attack in the last 12 months.

This report summarises the findings from a quantitative and qualitative survey with UK businesses on cyber security. The Department for Culture, Media and Sport (DCMS) commissioned the survey as part of the National Cyber Security Programme, following a previous comparable study by the Department published in 2016.[1] It was carried out by Ipsos MORI, in partnership with the Institute for Criminal Justice Studies at the University of Portsmouth, and comprised:

- a telephone survey of 1,523 UK businesses from 24 October 2016 to 11 January 2017[2]
- 30 in-depth interviews undertaken in January and February 2017 to follow up businesses that participated in the survey.

A copy of the main findings report, technical annex and other documents can be found on the GOV.UK website, at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017.

Code of practice for Official Statistics

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.

Acknowledgements

Ipsos MORI and DCMS would like to thank all the businesses and individuals who agreed to participate in the survey and those that provided an input into the survey's development. We would also like to thank the organisations who endorsed the fieldwork and encouraged businesses to participate, including the Association of British Insurers (ABI), the Confederation of British Industry (CBI), the Federation of Small Businesses (FSB), ICAEW and techUK.

Main findings

Businesses increasingly see cyber security as an important issue

The 2017 survey again highlights that virtually all UK businesses covered by the survey are exposed to cyber security risks. Since 2016, the proportion with websites (85%) or social media pages (59%) has risen (by 8 and 9 percentage points respectively), as has the use of cloud services (from 49% to 59%). This year's survey also establishes that three-fifths (61%) hold personal data on their customers electronically.

In this context, three-quarters (74%) of UK businesses say that cyber security is a high priority for their senior management, with three in ten (31%) saying it is a *very high* priority. The proportion noting it as a *very low* priority is lower than in 2016 (down from 13% to just 7%) – a change mainly seen among the micro and small business population.[3]

[1] See https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016 for the Cyber Security Breaches Survey 2016.

[2] This excludes sole traders, as well as agriculture, forestry and fishing businesses, and mining and quarrying businesses, which were outside the scope of the survey. The data is weighted to be representative of UK businesses by the remaining sizes and sectors.

[3] Micro businesses are those with 2 to 9 employees, small businesses those with 10 to 49 employees, medium businesses those with 50 to 249 employees, and large businesses those with 250 employees or more.

The survey highlights a range of factors that drive home the importance of cyber security for businesses, including:

- the specific threat of ransomware, which has underscored the value of any electronic data that businesses hold, not just personal or financial data
- having a senior individual in charge of cyber security – someone who can have direct contact with senior managers and can influence decision-making within the business
- board members being educated on the topic, enabling them to share knowledge and best practice across the different businesses they are involved in
- people being more exposed to cyber attacks, such as phishing scams, in their personal lives.

More businesses could still seek information or take further action to protect themselves

Three in five (58%) businesses have sought information, advice or guidance on the cyber security threats facing their organisations over the past year. The top specific sources of information mentioned are external security or IT consultants (32%) as well as online searches (10%). Only 4 per cent mention Government or other public sector sources, reflecting that awareness of the information and guidance offered by Government remains relatively low.

Despite this, three-quarters (75%) of those consulting Government sources say they found this material useful. The qualitative survey also shows once again that businesses tend to look to the Government as a trusted source to provide or signpost to information and guidance.

As in 2016, the majority of businesses (67%) have spent money on their cyber security, and this again tends to be higher among medium firms (87%) and large firms (91%).

Half of all firms (52%) have enacted basic technical controls across the five areas laid out under the Government-endorsed Cyber Essentials scheme.[4] Three-fifths (57%) have also attempted to identify cyber security risks to their organisation, for example through health checks or risk assessments (up from 51% in 2016). However, as in 2016, a sizable proportion of businesses still do not have basic protections or have not formalised their approaches to cyber security:

- Under two-fifths have segregated wireless networks, or any rules around encryption of personal data (37% in each case).
- A third have a formal policy that covers cyber security risks (33%), or document these risks in business continuity plans, internal audits or risk registers (32%).
- A third (29%) have made specific board members responsible for cyber security.
- A fifth (20%) of businesses have had staff attend any form of cyber security training in the last 12 months, with non-specialist staff being particularly unlikely to have attended.
- One-fifth (19%) are worried about their suppliers' cyber security, but only 13 per cent require suppliers to adhere to specific cyber security standards or good practice.

[4] These five areas include boundary firewalls and internet gateways, secure configurations, user access controls, malware protection, and patch management. See https://www.cyberaware.gov.uk/cyberessentials/.

- One in ten (11%) have a cyber security incident management plan in place.

All kinds of businesses continue to suffer from cyber security breaches with significant financial implications, but the reporting of breaches remains uncommon

Just under half (46%) of all UK businesses identified at least one cyber security breach or attack in the last 12 months. This rises to two-thirds among medium firms (66%) and large firms (68%).

Overall, businesses that hold electronic personal data on customers are more likely than average to have had breaches (51% versus 46%). Nonetheless, breaches are still prevalent among organisations whose senior managers consider cyber security a low priority (35%), and in firms where online services are not at all seen as core to the business (41%).

The most common types of breaches are related to staff receiving fraudulent emails (in 72% of cases where firms identified a breach or attack). The next most common related to viruses, spyware and malware (33%), people impersonating the organisation in emails or online (27%) and ransomware (17%). This highlights how, as well as having good technical measures in place, the awareness and vigilance of all staff are important to a business's cyber security.

The typical business is likely to only experience a handful of breaches in the space of a year, but a minority suffer considerably more. Across those that detected breaches, over a third (37%) report only being breached once in the year, but the same proportion say they were breached at least once a month, with 13 per cent saying it was daily. Moreover, in the last year, the average business identified 998 breaches – a figure pushed up by the minority of businesses that experience hundreds or thousands of attacks in this timeframe.

Not all breaches and attacks have material outcomes that affect the business. Nonetheless, four in ten (41%) businesses who identified a breach in the last 12 months – or a fifth (19%) of all UK businesses – report an outcome from cyber security breaches, such as a temporary loss of files or network access (23%) or systems becoming corrupted (20%). Six in ten (57%) of those who identified breaches also say the breach adversely impacted their organisation, for example through being forced to implement new protective measures (38%) or having staff time taken up dealing with the breach (34%).

Breaches frequently result in a financial cost to the business. Among the 46 per cent of businesses that detected breaches in the last 12 months, the survey finds that the average business faces costs of £1,570 as a result of these breaches. As in 2016, this is much higher for the average large firm, at £19,600, though the average medium firm (£3,070) and micro and small firms (£1,380) also incur sizeable costs.

Despite this, external reporting of breaches remains uncommon. Only a quarter (26%) reported their most disruptive breach externally to anyone other than a cyber security provider. The findings suggest that some businesses lack awareness of who to report to, why to report breaches, and what reporting achieves. Subsequent surveys will track whether reporting becomes more commonplace as businesses become increasingly aware of their cyber security risks and obligations.

Department for Culture Media & Sport

4th Floor, 100 Parliament Street
London, SW1A 2BQ
www.gov.uk/dcms