Press release: New figures show large numbers of businesses and charities suffer at least one cyber attack in the past year

- Over four in ten of all UK businesses suffered a breach or attack in the past 12 months.
- Most common attacks were fraudulent emails followed by cyber criminals impersonating an organisation online.
- Strong reminder to bosses to act ahead of new data protection laws coming into force on 25 May.

With one month to go until new data protection laws come into force, UK businesses are being urged to protect themselves against cyber crime after new statistics show over four in ten (43%) of businesses and two in ten charities (19%) suffered a cyber breach or attack in the past 12 months.

This figure rises to more than two thirds for large businesses, 72% of which identified a breach or attack. For the average large business the financial cost of all attacks over the past 12 months was £9,260 with some attacks costing significantly more.

The most common breaches or attacks were via fraudulent emails – for example, attempting to coax staff into revealing passwords or financial information, or opening dangerous attachments – followed by instances of cyber criminals impersonating the organisation online, then malware and viruses.

Minister for Digital and the Creative Industries, Margot James, said:

> We are strengthening the UK's data protection laws to make them fit for the digital age but these new figures show many organisations need to act now to make sure the personal data they hold is safe and secure.
>
> We are investing £1.9 billion to protect the nation from cyber threats and I would urge organisations to make the most of the free help and guidance available for organisations from the Information Commissioner's Office and the National Cyber Security Centre.

As part of the Government's Data Protection Bill, the Information Commissioner's Office (ICO) will be given more power to defend consumer interests and issue higher fines to organisations, of up to £17 million or 4 per cent of global turnover for the most serious data breaches. The new Bill requires organisations to have appropriate cyber security measures in place

to protect personal data.

The Government is introducing new regulations to improve cyber security in the UK's critical service providers in sectors such as health, energy and transport, and we have established the world-leading National Cyber Security Centre (NCSC) as part of plans to make the UK one of the safest places in the world to live and do business online.

Ciaran Martin, CEO of the NCSC, said:

> Cyber attacks can inflict serious commercial damage and reputational harm, but most campaigns are not highly sophisticated.
>
> Companies can significantly reduce their chances of falling victim by following simple cyber security steps to remove basic weaknesses. Our advice has been set out in an easy-to-understand manner in the NCSC's small charities and business guides.

The new statistics also show, among those experiencing breaches, large firms identify an average of 12 attacks a year and medium-sized firms an average of six attacks a year. Smaller firms are still experiencing a significant number of cyber attacks, with two in five micro and small businesses (42 per cent) identifying at least one breach or attack in the past 12 months, which could impact profits and reduce consumer confidence.

However, the survey shows more businesses are now using the Government-backed, industry-supported Cyber Essentials scheme, a source of expert guidance showing how to protect against cyber threats.

It shows three quarters of businesses (74 per cent) and more than half of all charities (53 per cent) say cyber security is a high priority for their organisation's senior management.

Organisations have an important role to play to protect customer data. Small businesses and charities are urged to take up tailored advice from the National Cyber Security Centre. Larger businesses and organisations can follow the Ten Steps to Cyber Security for a comprehensive approach to managing cyber risks and preventing attacks and data breaches.

Organisations can also raise their basic defences and significantly reduce the return on investment for attackers by enrolling on the Cyber Essentials initiative and following the regularly updated technical guidance on Cyber Security Information Sharing Partnership and the NCSC website.

Information Commissioner, Elizabeth Denham, said:

"Data protection and cyber-security go hand in hand: privacy depends on security.

“With the new data protection law, the General Data Protection Regulation (GDPR) taking effect in just a few weeks, it’s more important than ever that organisations focus on cyber-security. That’s why we’ve been working with the Department for Culture Media and Sport (DCMS) and the National Cyber Security Centre (NCSC) to offer practical security steps that organisations can consider to keep data safe.

“We understand that there will be attempts to breach systems. We fully accept that cyberattacks are a criminal act. But we also believe organisations need to take steps to protect themselves against the criminals. I’d encourage organisations to use the new regulations as an opportunity to focus on data protection and data security.

“Increasing the public’s trust and confidence in the way people’s data is handled is our priority and good data protection practice will go some way to making the UK the safest place to be online.”

Organisations which hold and process personal data are urged to prepare and follow the [guidance and sector FAQS](https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/ freely available from the Information Commissioner’s Office. Its dedicated advice line for small organisations has received more than 8000 calls since it opened in November 2017, and the Guide to the GDPR has had over one million views. The regulator also has a GDPR checklist, and 12 steps to take now to prepare for GDPR.

The survey also revealed:

*Larger businesses and charities are more likely than the average to identify cyber attacks. Breaches were more likely to be found in organisations that hold personal data and where employees use their own personal devices for work.

*A huge proportion of all organisations are still failing to get the basics right. A quarter (25 per cent) of charities are not updating software or malware protections (27 per cent) and a third of businesses (33%) do not provide staff with guidance on passwords.

*More than one in 10 (11 per cent) of large firms are still not taking any action to identify cyber risks, such as health checks, risk assessments, audits or investing in threat intelligence.

Notes to editors:

*Media enquiries – please contact the DCMS News and Communications team on 020 7211 2210. Read the Cyber Security Breaches Survey 2018.

*The Cyber Security Breaches Survey 2018 was carried out for DCMS by Ipsos MORI, in partnership with the Institute for Criminal Justice Studies at the University of Portsmouth. A telephone survey of 1,519 UK businesses (excluding agriculture, forestry and fishing businesses) and 569 UK registered charities was undertaken from 9 October 2017 to 14 December 2017. The business sample included 1.004 micro and small firms (with 1 to 49

staff), 263 medium firms (with 50 to 249 staff) and 252 large firms (with 250 or more staff). The data have been weighted to be statistically representative of these two populations.

*Full survey findings and technical details can be found on this page.

*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.

*The Cyber Security Breaches Survey 2018 was carried out for DCMS by Ipsos MORI, in partnership with the Institute for Criminal Justice Studies at the University of Portsmouth. A telephone survey of 1,519 UK businesses (excluding agriculture, forestry and fishing businesses) and 569 UK registered charities was undertaken from 9 October 2017 to 14 December 2017. The business sample included 1,004 micro and small firms (with 1 to 49 staff), 263 medium firms (with 50 to 249 staff) and 252 large firms (with 250 or more staff). The data have been weighted to be statistically representative of these two populations.

*The Cyber Security Breaches Survey comes on the back of recent Government action to boost cyber security, including:

*Announcing a new £13.5 million cyber innovation centre, located in the Queen Elizabeth Olympic Park, to help secure the UK's position as a global leader in the growing cyber security sector.

*The Government is encouraging all firms to act: the 10 Steps to Cyber Security provides advice to large businesses, and the Cyber Essentials scheme is available to all UK firms and charities. The Cyber Aware campaign aims to drive behaviour change amongst small businesses and individuals, so that they adopt simple secure online behaviours to help protect themselves from cyber criminals.

*Ipsos MORI surveyed 1,519 UK businesses and 569 UK registered charities by telephone from 9 October 2017 to 14 December 2017.

*The proportions of medium and large businesses achieving the Cyber Essentials standards have risen steadily since 2016 – up from 4 per cent to 13 per cent of medium businesses and from 10 per cent to 25 per cent of large businesses.

*The survey found 38% of businesses and 44% of charities (surveyed between October and December 2017) had heard of the new incoming data protection laws. Of those aware, 27% of businesses and 26% of charities had made changes to their operations as a result. Of these, just under half of those businesses and over one third of charities, made changes to their cyber security practices.