

Press release: Almost half of UK firms hit by cyber breach or attack in the past year

- Firms holding personal data more likely to be attacked
- Most common attacks were fraudulent emails, followed by viruses and malware

The [Cyber Security Breaches Survey 2017](#) reveals nearly seven in ten large businesses identified a breach or attack, with the average cost to large businesses of all breaches over the period being £20,000 and in some cases reaching millions. The survey also shows businesses holding electronic personal data on customers were much more likely to suffer cyber breaches than those that do not (51 per cent compared to 37 per cent).

The most common breaches or attacks were via fraudulent emails – for example coaxing staff into revealing passwords or financial information, or opening dangerous attachments – followed by viruses and malware, such as people impersonating the organisation online and ransomware.

Businesses also identified these common breaches as their single most disruptive breach, and the vast majority of them could have been prevented using the Government-backed, industry supported Cyber Essentials scheme, a source of expert guidance showing how to protect against these threats.

These new statistics show businesses across the UK are being targeted by cyber criminals every day and the scale and size of the threat is growing, which risks damaging profits and customer confidence.

The Government has committed to investing £1.9 billion to protect the nation from cyber attacks to help make the UK the safest place to live and do business online.

Business also has a role to play to protect customer data. The government offers free advice, online training and Cyber Essentials and Cyber Aware schemes.

The survey also revealed:

Of the businesses which identified a breach or attack, almost a quarter had a temporary loss of files, a fifth had software or systems corrupted, one in ten lost access to third party systems they rely on, and one in ten had their website taken down or slowed.

Firms are increasingly concerned about data protection, with the need to protect customer data cited as the top reason for investing by half of all firms who spend money on cyber security measures.

Following a number of high profile cyber attacks, businesses are taking the

threat seriously, with three quarters of all firms saying cyber security is a high priority for senior managers and directors; nine in ten businesses regularly update their software and malware protection; and two thirds of businesses invest money in cyber security measures.

Small businesses can also be hit particularly hard by attacks, with nearly one in five taking a day or more to recover from their most disruptive breach.

Areas where industry could do more to protect itself include around guidance on acceptably strong passwords (only seven in ten firms currently do this), formal policies on managing cyber security risk (only one third of firms), cyber security training (only one in five firms), and planning for an attack with a cyber security incident management plan (only one in ten firms).

All businesses which hold personal data will have to make sure they are compliant with the new General Data Protection Regulation (GDPR) legislation from May 2018. This will strengthen the right to data protection, which is a fundamental right, and allow individuals to have trust when they give their personal data.

The Cyber Breaches Survey is part of the Government's five-year National Cyber Security Strategy to transform this country's cyber security and to protect the UK online. As part of the strategy, the Government recently opened the new National Cyber Security Centre (NCSC), a part of GCHQ.

One of the key objectives of the NCSC is to increase the UK's cyberspace resilience by working with and providing expert advice tailored to organisations and businesses in every sector of the UK economy and society.

Ciaran Martin, CEO of the National Cyber Security Centre, said:

UK businesses must treat cyber security as a top priority if they want to take advantage of the opportunities offered by the UK's vibrant digital economy.

The majority of successful cyber attacks are not that sophisticated but can cause serious commercial damage. By getting the basic defences right, businesses of every size can protect their reputation, finances and operating capabilities.

Cyber Essentials, technical advice on CiSP and regularly updated guidance on the NCSC website offers companies, big and small, simple steps that can significantly reduce the risk of a successful attack.

ENDS

Notes to editors:

1. Read the [Cyber Security Breaches Survey 2017](#)
2. 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.
3. The survey was carried out by Ipsos MORI in partnership with the Institute for Criminal Justice Studies at the University of Portsmouth.
4. The survey fieldwork has been endorsed by the Association of British Insurers (ABI), the Confederation of British Industry (CBI), the Federation of Small Businesses (FSB), ICAEW and techUK.
5. Media enquiries – please contact the DCMS News and Communications team on 020 7211 2210 or out of hours on 07699 751153.
6. The Cyber Security Breaches Survey comes on the back of recent Government action to boost cyber security, including:
 - Strengthening the Cyber Essentials scheme, which protects organisations against the most common online threats. A number of large firms, such as BT, Airbus, Vodafone, Astra Zeneca and Barclays, are also encouraging their suppliers to adopt the scheme.
 - New measures to support the UK's £22 billion cyber security industry, including boosting the cyber ecosystem by helping academics commercialise their research and funding an early stage accelerator programme.
 - Funding Academic Centres of Excellence to specialise in developing the latest cyber security techniques and contribute to the UK's increased knowledge and capability in this field.
 - Working to develop cyber innovation centres in London and Cheltenham to support entrepreneurs and innovators to develop new cyber security products and businesses.
 - Developing the cyber security skills pipeline so the UK has the people it needs now and in the future, including a cyber security apprenticeships scheme, a cyber schools programme and a cyber retraining programme to help fast-track professionals into the industry.
 - The popular CyberFirst programme is inspiring, encouraging and developing a cyber-savvy cohort of students to help protect the UK's digital society.
 - 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. The Cyber Aware scheme (formerly Cyber Streetwise) 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.

7. 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.
-

[News story: Making energy clean, affordable and secure: apply for funding](#)

Businesses can apply for a share of £13 million for innovative projects that address the issues of cost, emissions and security of supply.

The Energy Catalyst has up to £13 million to support innovative market-focused projects in the energy sector both in the UK and in developing countries.

This competition is cofunded by the [Department for International Development](#), the [Department for Business, Energy & Industrial Strategy](#) and the [Engineering and Physical Sciences Research Council](#). It is being run by Innovate UK.

Rapid change in energy systems

Energy systems around the world are facing rapid change. There is a clear need to address the challenge of providing energy that is clean, affordable and secure at the same time.

The competition aims to help UK businesses to grasp the opportunities on offer through meeting the challenges facing the energy sector. There are 3 types of award for projects that are at an early, mid or late stage of development.

This is the fifth round of the Energy Catalyst. More than 200 projects with a

total value of £200 million have already been funded in the previous 4 rounds.

Competition information

- this competition opens on 24 April 2017, and the deadline for registration is midday on 21 June 2017
 - the competition is open to any UK organisation and may involve international partners
 - research organisations may lead early stage projects but all projects must include a business. Mid-stage and late-stage projects must be led by a business working with at least one partner
 - project costs can vary between £50,000 and £10 million depending on the stage and can last between 1 and 3 years
 - businesses can attract up to 70% of their project costs
 - briefing events will be held in London, Birmingham and Glasgow in April and May 2017
-

[News story: Autonomous supply to military front line: apply for contracts](#)

Businesses can apply for a share of up to a possible £3 million for supplying the military front line through autonomous systems

The [Ministry of Defence](#) is to invest in projects that look at ways of using autonomous systems in the 'last mile' of the supply chain to front-line military operations.

Up to £1.5 million is available in the first phase of the competition. There is up to an additional £1.5 million in phase 2 that includes proposed system designs. This will only be available to projects funded through phase 1.

A third phase could include a longer period of trials and evaluation of promising proposals.

Last mile supply

Last-mile resupply involves delivery of combat materials from a physical base or logistics vehicle and is often challenging because of the hostile and contested environment. Although described as last-mile, real-life distances could be up to 30km in some instances.

Current ways of supplying the front line involve transport aircraft,

helicopters, large trucks, trailers with quad bikes and soldiers on foot.

The challenge areas

This funding competition is particularly looking for solutions in 3 challenge areas:

- unmanned air and ground load-carrying platforms
- technologies and systems that allow load-carrying platforms to operate autonomously
- technologies to autonomously predict, plan, track and optimise re-supply demands from military users

The competition is for fully funded contracts under SBRI (Small Business Research Initiative).

Competition information

- the competition is open, and the deadline for applications is midday on 21 June 2017
- the competition is for fully funded development contracts
- phase 1 contracts are likely to be worth between £40,000 and £80,000 and last up to 6 months
- a networking event for potential applicants will take place on 23 May 2017
- there will be a webinar for potential applicants on 30 May 2017

[Notice: Funding competition: energy catalyst round 5](#)

Updated: Added link to register for brokerage event in London with DFID. Added link to recorded briefing and supporting materials.

The [Department for International Development](#) (DFID), the [Department for Business, Energy & Industrial Strategy](#) (BEIS) and the [Engineering and Physical Sciences Research Council](#) (EPSRC) are to invest up to £13 million in innovation projects to address the global need for clean, affordable and secure energy.

The aim of the Energy Catalyst competition is to support highly innovative, market-focused energy solutions in any technology or sector or international market.

Proposals must address all 3 elements of the energy trilemma:

- cost
- emissions
- security of supply

The competition is open to any UK organisation and may also include international partners. You should apply into the stream most closely aligned with your project. Universities and small and medium-sized enterprises (SMEs) are encouraged to apply. Research organisations may lead early-stage feasibility projects.

There are 3 options to apply into this competition. These are referred to as streams and will be run in parallel. The streams are dependent on the stage your project is at:

- early stage
- mid-stage
- late stage

You should choose the stream that broadly reflects the technical and commercial readiness of your project.

Early-stage competition stream

These are technical feasibility projects. Projects can last up to 1 year, with total costs ranging from £50,000 to £300,000. Research organisations may lead early-stage projects, in partnership with at least one UK business. UK SMEs can lead early-stage projects with or without partners.

Mid-stage competition stream

These are industrial research projects. Projects can last up to 3 years, with total costs ranging from £50,000 to £1.5 million. Mid-stage projects must be collaborative and led by a UK business.

Late-stage competition stream

These are experimental development projects. Projects can last up to 3 years, with total costs ranging from £50,000 to £10 million. Late-stage projects must be collaborative and led by a UK business.

All projects must include at least one UK business. We expect most projects to start on 1 January 2018.

The competition opens on 24 April 2017.

You must register before midday on 21 June 2017.

You must apply before midday on 28 June 2017.

[Watch the competition briefing webinar](#) or [view the event materials](#) and

[presentation](#).

Attend one of the brokerage events in:

[London](#)

[Birmingham](#)

[Glasgow](#)

[London](#) (with DFID)

[Register and apply online](#).

Not right for your innovation project? View other [Innovate UK funding competitions](#).

[News story: Encouraging cycling and walking: apply for business funding](#)

Updated: Removed information on briefing webinar due to cancellation.

Up to £470,000 is available for organisations with innovative projects that lead to people walking and cycling more. Innovations may include technology, infrastructure, manufacturing or behavioural change.

This is a [Small Business Research Initiative](#) (SBRI) competition. It has 2 phases. Up to £170,000 is available for phase 1, and up to £300,000 for phase 2.

Natural choice for shorter journeys

The government's vision is for cycling and walking to become the natural choice for shorter journeys. The [Department for Transport](#) (DfT) is funding this competition and is inviting proposals which:

- remove current barriers to walking and cycling
- encourage people to make more journey stages to by bicycle or on foot

Removing the barriers

To meet these aims, DfT intends to focus on:

- better safety – safety and safety perceptions are among the biggest barriers for people wanting to take up cycling and walking
- better mobility – to make cycling and walking normal, easy and enjoyable, we need better links and networks to key destinations
- better streets – well-designed and accessible streets can encourage people to walk or cycle more as part of their daily routine

Competition information

- this competition opens on Wednesday 19 April 2017, and the deadline for registration is midday on 7 June 2017
- this competition is open to individuals, groups and organisations, but is particularly suitable for early-stage, small and medium-sized enterprises (SMEs)
- industry partners such as local government, independent and third sectors can carry out the project on their own or with others
- total project costs can vary between £25,000 and £100,000 and up to 15 weeks to up to 9 months, depending on the phase

[Find out more about this competition and apply online.](#)