2016 CYBER SECURITY BREACHES SURVEY

Crendon Insurance Brokers

The internet promises big rewards for businesses but also big risks.

The threat is significant—24 per cent of all businesses detected one or more cyber security breaches in the last 12 months. But that number skyrockets when classifying businesses by size—jumping to 51 per cent of all medium firms and 65 per cent of all large firms. The same holds true for the cost of breaches—the average cost of all breaches over the last 12 months was £3,480 while the most costly breach identified was £3 million.

Businesses understand that the threat is significant, but there is a serious gap between awareness and action—only 51 per cent of all businesses have attempted to identify their unique cyber risks, while 69 per cent of all businesses say cyber security is either a very high or fairly high priority for their organisation's senior management.

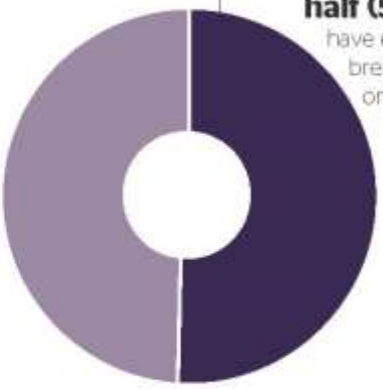
With that gap in mind, **Crendon Insurance Brokers Ltd** is proud to present our report summarising the 2016 Cyber Security Breaches Survey for the United Kingdom, commissioned by the Department for Culture, Media & Sport as part of the National Cyber Security Programme. As Britain becomes ever more reliant on the internet for commerce and contact, prudent business owners would do well to scrutinise their cyber security processes. Indeed, the United Kingdom is the biggest internet shopper in Europe, with 80 per cent of people buying something online in the past year. And, e-commerce sales have surged from £335 billion for non-micro businesses in 2008 to £573 billion in 2014—a 71 per cent increase in only six years. Don't miss out on the expansive opportunities of selling online, or resign your business to cyber attacks and breaches because you failed to value cyber security. Businesses can protect themselves and ensure online success with simple, vigilant cyber risk management guidance, available from Crendon Insurance Brokers Ltd today.

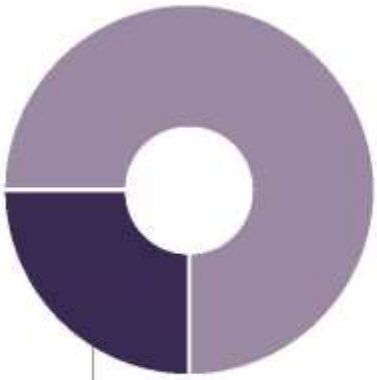
As you read through these numbers, consider what you can do to bolster your business' cyber security and ensure your future success.

INCIDENCE AND IMPACT OF BREACHES

Experience of Breaches

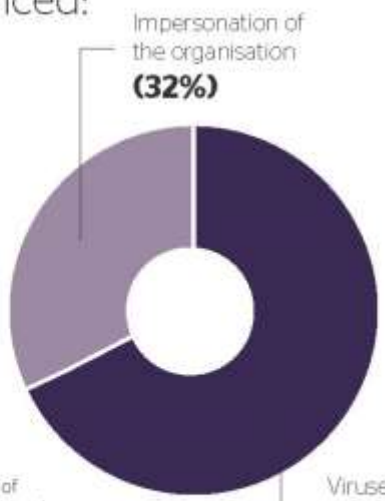
24% of all businesses have experienced one or more cyber security breaches in the **last 12 months**—this is substantially higher among **medium firms (51%)** and **large firms (65%)**.





25% of large organisations that have had breaches have experienced them at least once per month.

Most common types of breaches experienced:



*Typically the types of breaches that cause most disruption to businesses

Sectors most likely to experience certain types of breaches:

Information, communications or utility firms were more likely to have breaches relating to personally owned devices **(19% versus 8% of all businesses).**

Administration or real estate firms were more likely to suffer from viruses, spyware or malware **(77% versus 68%).**

Financial services firms were more likely to suffer from impersonation in emails or online **(60% versus 32%).**

INCIDENCE AND IMPACT OF BREACHES CONTINUED

Time Taken to Recover from Breaches

78% of businesses that had experienced breaches in the last 12 months took less than one day to recover from their most disruptive breach.

Large firms lose the most time on average when dealing with breaches: **4.3 days lost** dealing with the most disruptive breach of **last 12 months** (compared to 2.3 days on average overall).

Micro firms took longer: **24%** (versus 14% overall) said it took up to one week to recover from their most disruptive breach.

FINANCIAL COST OF BREACHES

Estimated average cost of all breaches over the last 12 months:

£3,480

This is much higher for large firms:

£36,500

Estimated average cost of the single most disruptive breach from the last 12 months:

£2,620
across all businesses
£32,300
for large businesses

Most costly single breach captured in this survey:

£3 million

Cyber breaches have expansive knock-on effects: Businesses face various barriers to accurate financial monitoring, and may therefore underestimate the costs they do and will incur from cyber security breaches.

IMPORTANCE OF CYBER SECURITY TO BUSINESSES

Action Taken (or Lack of)

70% say that cyber security is either a **very high (33%)** or **fairly high (37%)** priority for their organisation's senior management.

Only **51%** of all businesses have attempted to identify the cyber security risks faced by their organisation.

This is higher amongst **medium firms (78%)** and **large firms (94%)**.

Only **29%** have written cyber security policies, and only **13%** set minimum cyber security standards for their suppliers

26% of businesses report that their senior managers are never updated on any cyber security actions.

Only **34%** of companies have rules specifically on personal data encryption, despite it being at the centre of various high-profile cyber security breaches.

Awareness of Government Cyber Security Initiatives

Only 11% of all businesses are aware of Government's 10 Steps To Cyber Security guidance (click here for more information).

Only 6% of all businesses are aware of the Cyber Essentials Scheme, the Government-backed scheme to guide businesses in protecting themselves against cyber threats (click here for more information).

APPROACHES TO CYBER SECURITY

68% of all firms have some level of cyber security spend, spending an average of **£4,060** in the last financial year.

Staff Approaches to Cyber Security

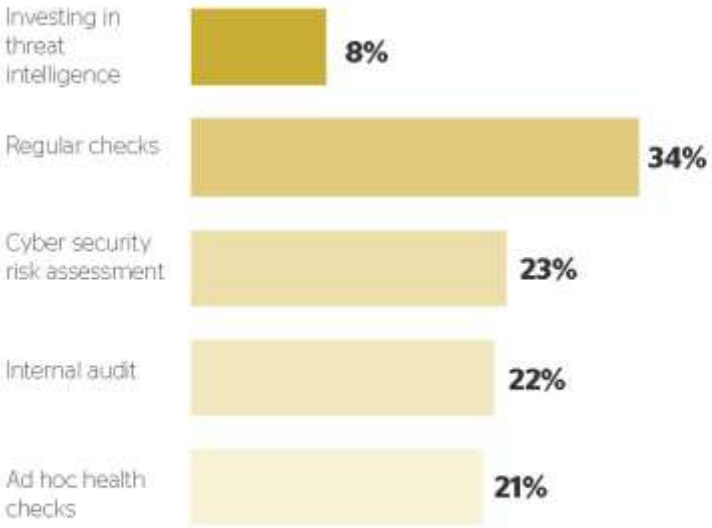
34% of businesses employ staff whose job role specifically includes information security or governance

Only **17%** of businesses have required staff to attend cyber security training in the last 12 months.

Risk Management

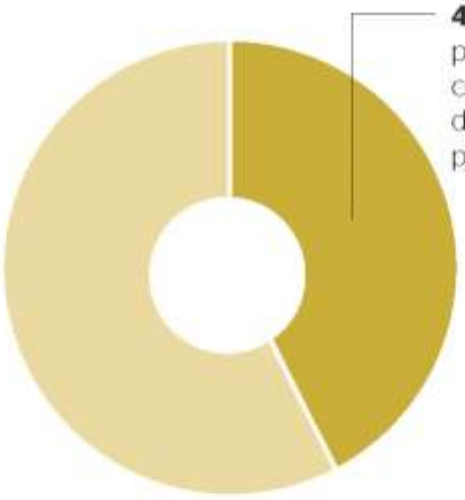
51% of all businesses have taken some form of action to identify cyber security risks.

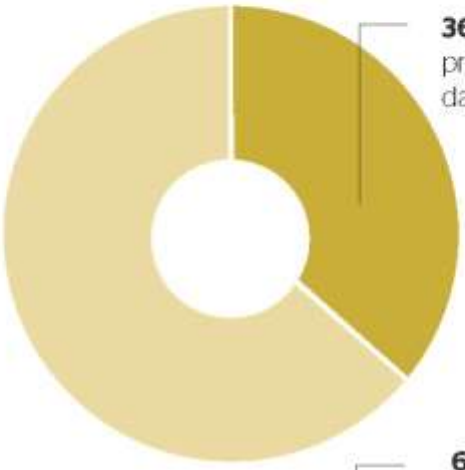
The most common actions taken by all businesses to identify cyber security risks:

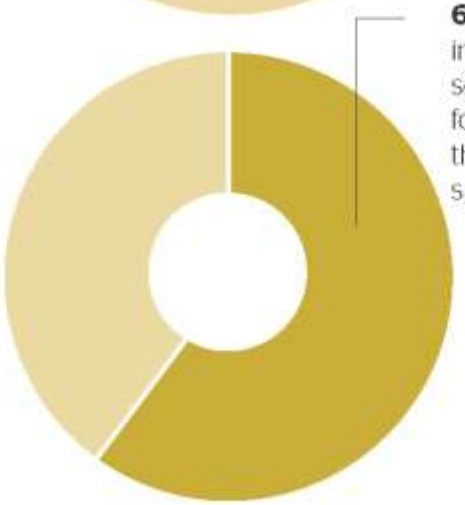


Drivers of Investment

Why businesses invest in cyber security:

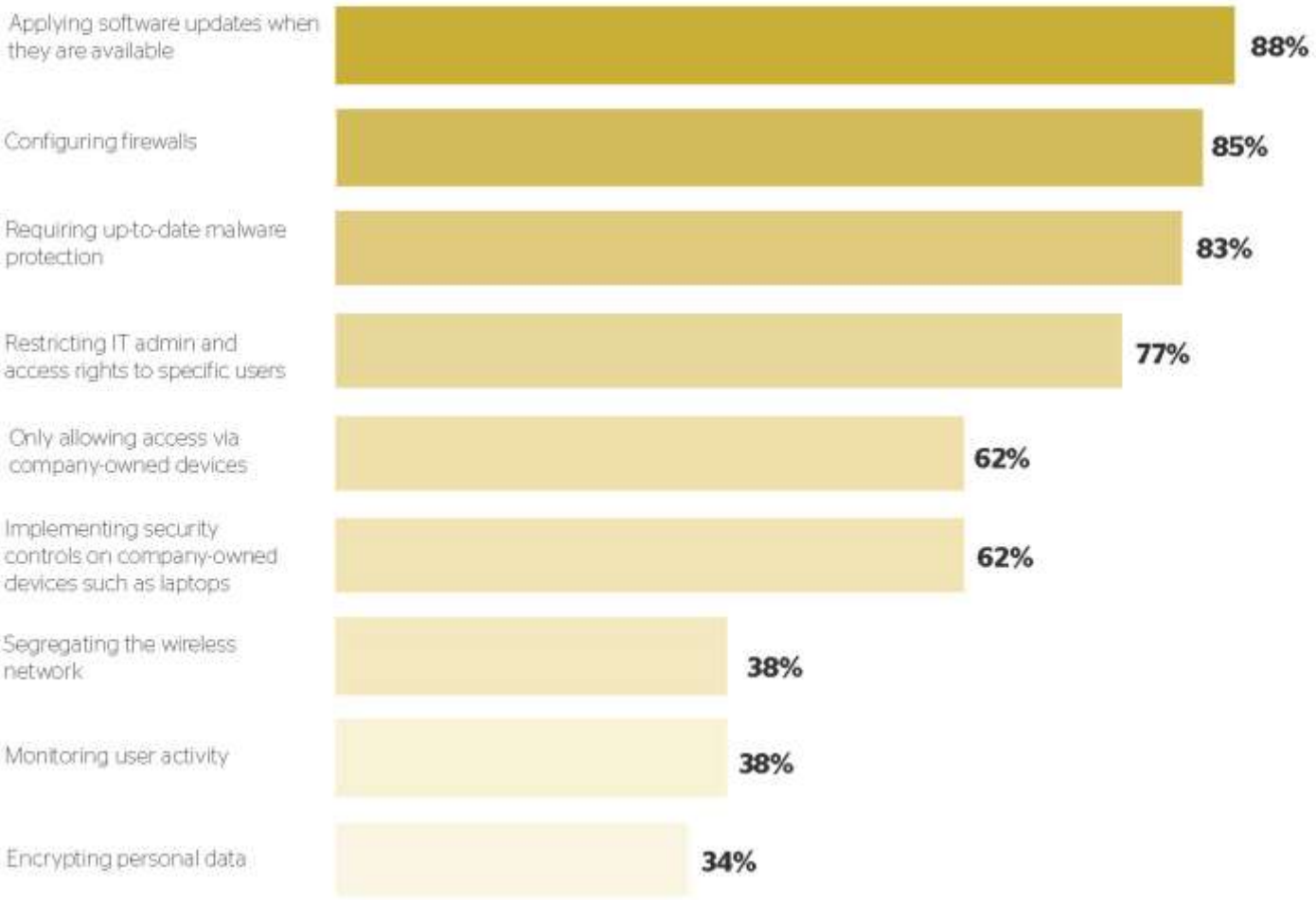




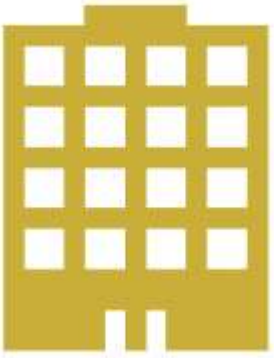


APPROACHES TO CYBER SECURITY CONTINUED

Rules Businesses Have Implemented to Manage Cyber Risks



Implementing Government Cyber Security Initiatives

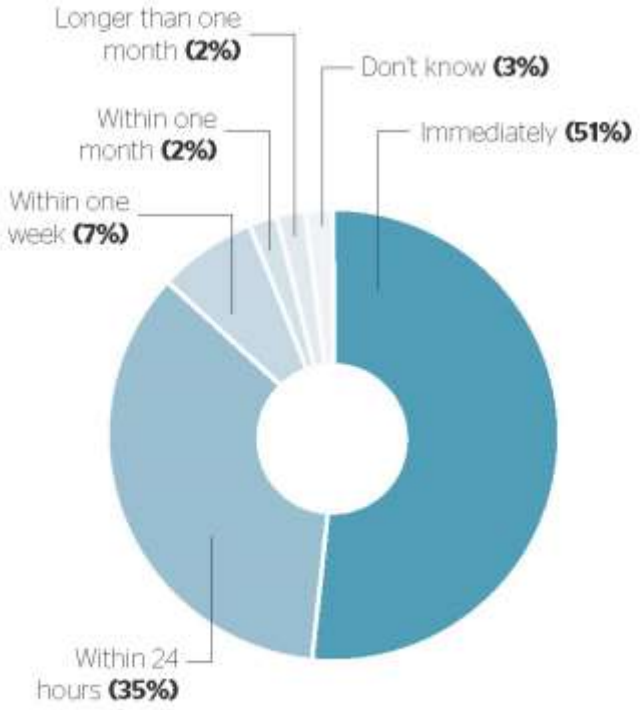


48% of all firms, including **76% of medium** and **87% of large firms** say they have equivalent of Government's Cyber Essentials scheme in place, but most may not currently realise that they can therefore be certified in the scheme.

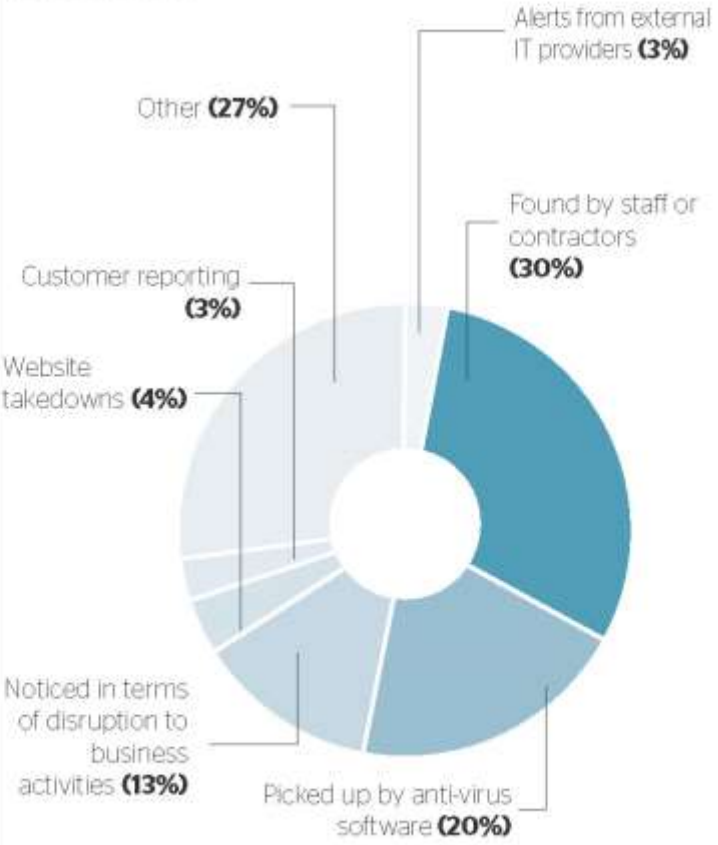
Only **2%** of all businesses have formally implemented Cyber Essentials standards across their organisation.

DEALING WITH BREACHES

Amount of time taken to identify most disruptive breach of last 12 months:

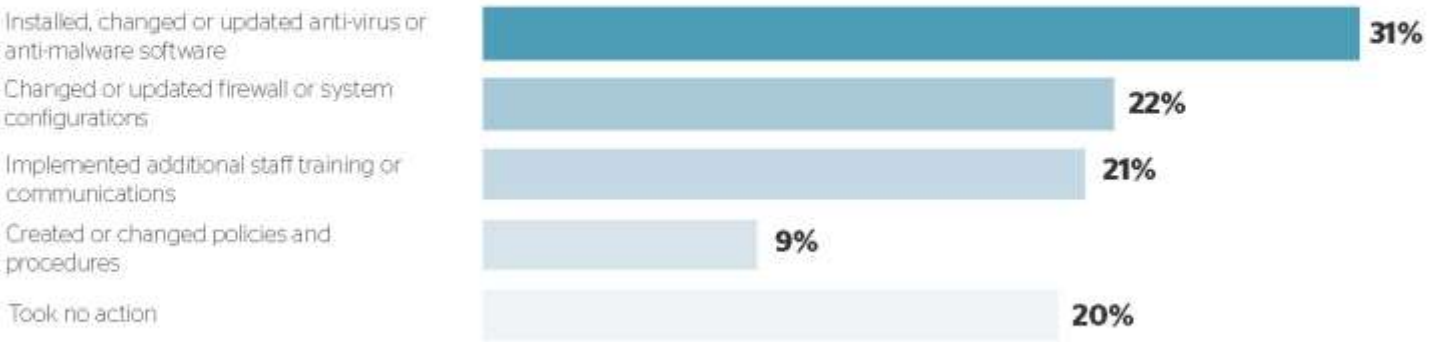


How the most disruptive breach was identified:



Preventing Future Breaches

The most common actions following the most disruptive breach of the last 12 months:



DEALING WITH BREACHES CONTINUED

Understanding Breaches

61% of businesses consider their most disruptive breaches to have been intentional

26% consider their most disruptive breaches to have been accidental

39% of businesses do not know what factors contributed to the most disruptive attack or breach occurring.

Most common factor identified by all businesses is human error **(14%)**

52% of businesses do not know the source of the most disruptive breach or attack.

Most common source identified by all businesses is email attachments or websites **(28%)**

THE VALUE AND IMPORTANCE OF CYBER SECURITY INSURANCE

Government research suggests that cyber insurance can provide solutions for the following range of cyber risks:

Privacy events

(expenses related to responding to a data breach and third-party liabilities)

Network business interruption

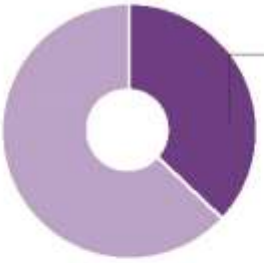
Network security liability

Physical asset damage

Data and software damage

Reputational damage

Cyber crime



Cyber extortion

Percentage of businesses with cyber insurance, by size: