cyber risk
statistics 2021

Hine®
CHARTERED INSURANCE BROKERS

Cybercrime is not going away any time soon.

The evidence suggests that the effects of COVID-19 have made the risk level of experiencing an attack higher than ever, and the resulting costs are substantial.

As we become increasingly reliant on technology, at times solely, now's the time for businesses to take action against cybercrime before it's too late.

The benefits of cyber insurance

Due to the evolving methods of cybercriminals, it's near enough impossible to fully safeguard your business with cybersecurity software alone. That's why it's not only important to remain vigilant in your defence against an attack, but also to have a plan of action in place should you become victim to one.

Standard Business Insurance doesn't adequately protect your business against cyberattacks, especially when it comes to your data. With dedicated Cyber Insurance in place, your business will have the reassurance that you're covered for the aftermath of an attack, including damage to your IT systems, business interruption, data loss, reputational damage and more.

The true risk of cybercrime

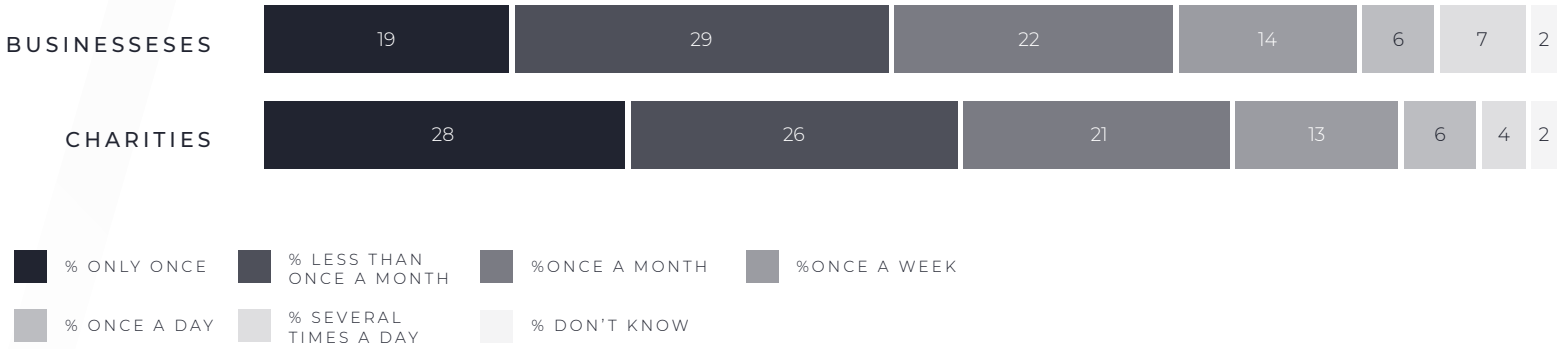
In this document, we have gathered the latest Government statistics surrounding cybercrime to demonstrate the extent of the risks that your business faces.

The threat to businesses

Over the past 12 months, 39% or four in 10 of all business have suffered from a cyberattack. While this figure is down from the previous year – due to the number of businesses remaining closed over the pandemic – the threat level is not thought to be any lower than the previous years.

Frequency of attacks

Among those who experienced a cyberattack over the past year, almost half of businesses (49%) and 44% of charities said this happened at least once a month. Around a quarter experienced an attack once a week.

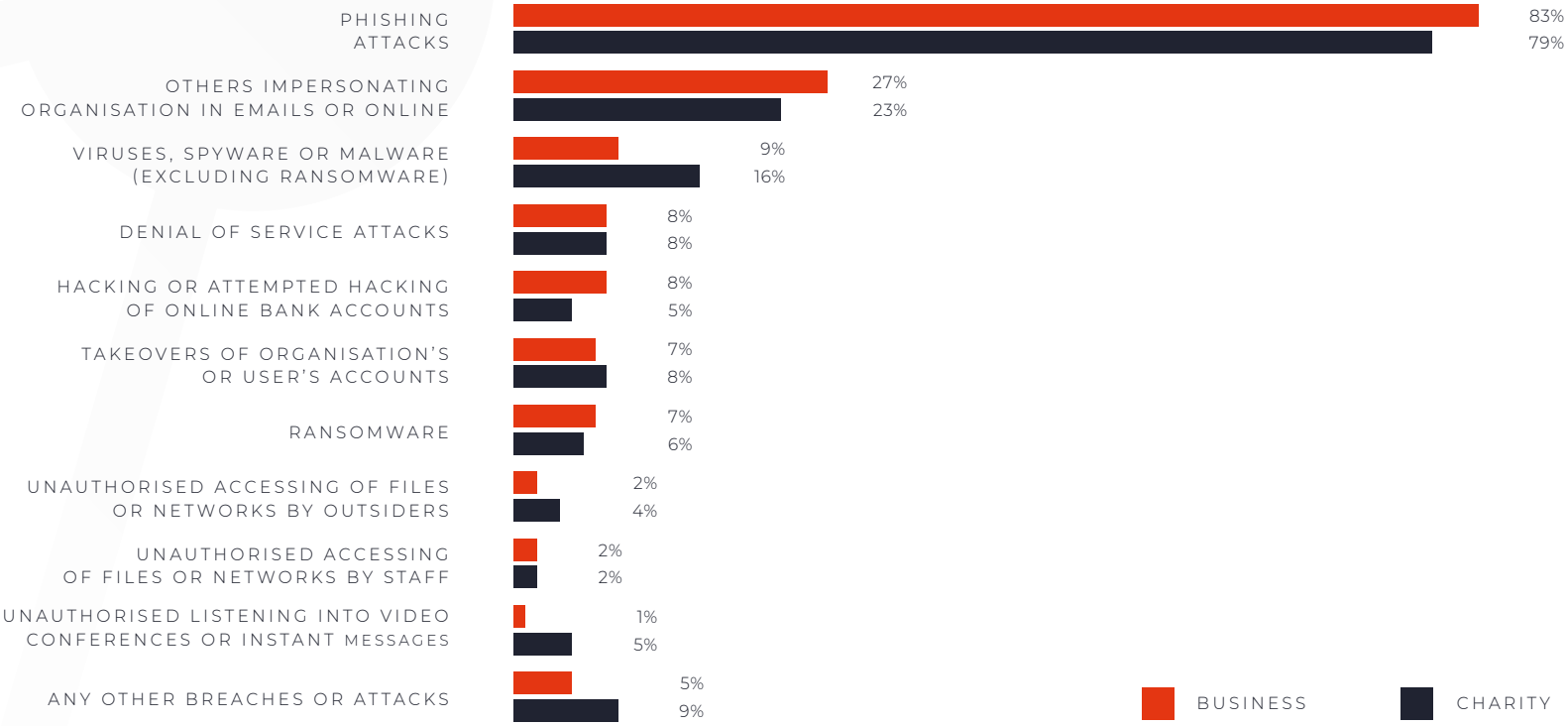


The information on this page has been extracted from the latest Government Cyber Security Breaches Survey 2021 conducted by the Department for Digital, Culture, Media and Sport.

What are the most frequent cyberattacks?

While the most common types of attacks by far are phishing, staff receiving fraudulent emails or being directed to fraudulent websites, there are a number of directions in which a business or charity may be attacked from.

Find out the most frequent attacks for both businesses and charities below:



What are the most frequent cyberattacks?

The evolution of cyberattacks

Since 2017, the most frequent type of attacks have evolved from direct malware to phishing. Yet, the three most common attacks

- phishing, others impersonation organisations in emails or online, and viruses, spyware or malware (excluding ransomware)
- have remained consistent. This allows businesses to pinpoint methods to prevent such incidents, including frequent staff training, dedicated IT support, security software and tailored insurance.

Among those businesses identifying any breaches or attacks, from 2017 to 2021 there has been:

- A rise in phishing attacks from 72% to 83%
- A fall in viruses or other malware from 33% to 9%
- A fall in ransomware from 17% to 7%

The information on this page has been extracted from the latest Government Cyber Security Breaches Survey 2021 conducted by the Department for Digital, Culture, Media and Sport.

The cost to businesses

While not every cyberattack will have financial repercussions for your business, if it does have a material outcome, the figure that you owe may quickly rise into the thousands.

While the results below detail the average costs to businesses, there have been a number of cases where companies have needed to pay much more.

Average cost of breaches across different sized businesses

Among those who experienced a cyberattack over the past year, almost half of businesses (49%) and 44% of charities said this happened at least once a month. Around a quarter experienced an attack once a week.

Average cost of all breaches or attacks identified in the last 12 months

	ALL BUSINESSES	MICRO/SMALL BUSINESSES	MEDIUM/LARGE BUSINESSES	ALL CHARITIES
Across organisations identifying any breaches or attacks				
MEAN COST	£2,670	£2,600	£3,930	£2,110
MEDIAN COST	£0	£0	£96	£0
TOTAL BUSINESSES/CHARITIES PARTICIPATING	623	360	263	171
Only across organisations identifying breaches with an outcome				
MEAN COST	£8,460	£8,170	£13,400	TOO FEW CHARITIES TO ANALYSE
MEDIAN COST	£500	£500	£2,280	
TOTAL BUSINESSES/CHARITIES PARTICIPATING	143	74	69	

Has the cost of cyberattacks increased over the years?

Compared with previous years, these figures suggest that when a cyberattack does have a material outcome for a business, the potential costs have risen significantly. This applies to firms of all sizes, from large corporations to small local businesses.

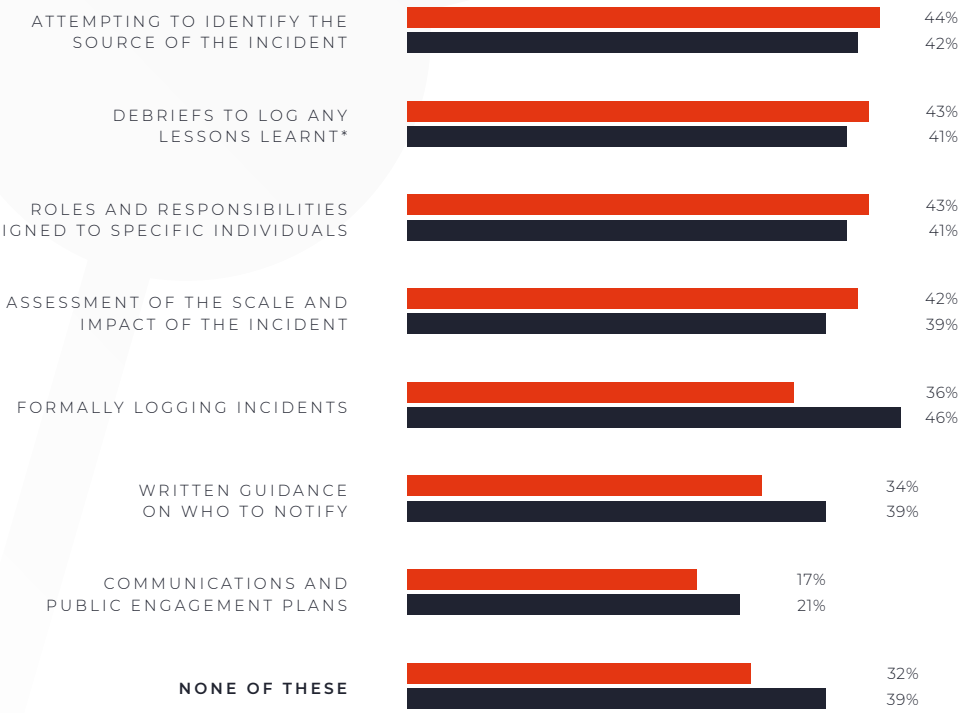
It has also been found that the costs in the aftermath of a cybersecurity incident are much higher than the immediate direct cost to an organisation. The indirect costs are on par with the direct costs.

The information on this page has been extracted from the latest Government Cyber Security Breaches Survey 2021 conducted by the Department for Digital, Culture, Media and Sport.

The aftermath of a breach

The way a business responds to a cyberattack is essential to ensuring that due diligence has been met and in safeguarding itself against future incidents. The majority of businesses (66%) do have some type of formalised response in an incident; however, it often isn't comprehensive which could result in repercussions from regulatory bodies and similar cases reoccurring in the future.

Cyber response measures:



Participants: 1,419 UK businesses; 487 charities
*New code for 2021

The information on this page has been extracted from the latest Government Cyber Security Breaches Survey 2021 conducted by the Department for Digital, Culture, Media and Sport.

The aftermath of a breach

Internal reporting to senior staff

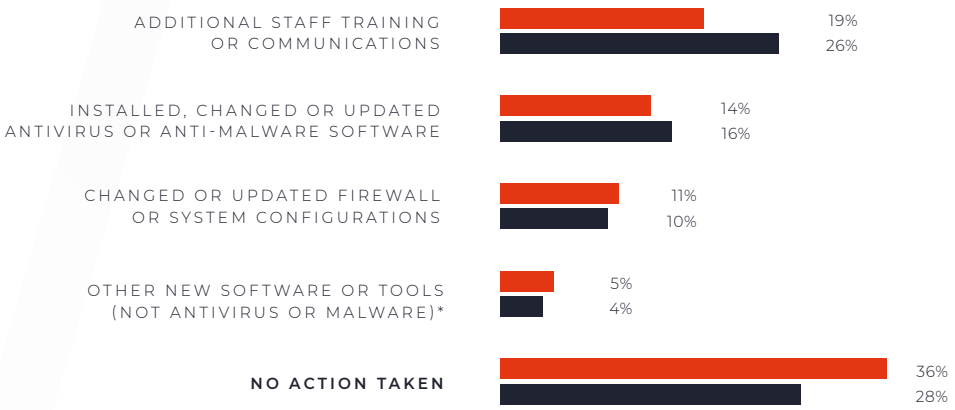
Having experienced a breaches or attack, the vast majority (93%) of businesses informed their senior managers or directors of their most disruptive breach.

External reporting

In comparison, external reporting of breaches hasn't received the same due diligence. Only two-fifths of businesses (37%) and three in 10 charities (28%) reported their most disruptive breach outside of their organisation.

Actions taken to prevent future breaches or attacks

Following an attack, the majority of businesses (62%) and charities (69%) took action to prevent further breaches. However, approximately one-third of businesses (36%) and one quarter of charities (28%) have taken no action since their most disruptive breach.



Participants: 627 businesses that recalled their most disruptive breach or attack in the last 12 months; 182 charities
*New code for 2021

Protect your digital assets with cyber insurance

As your broker, our top priority is ensuring that should the worst happen, your business or personal property is covered. We do all we can to help you to prevent any risks from occurring, but even with the best will in the world it's impossible to prepare for absolutely everything. With the right cover however, you can put thorough protection in place.

With cyber and data cover being such a new insurance product, we know that some of our customers may have questions. Please take a look at some FAQs below, and if you have any more specific queries, just pick up the phone and speak to us.

Why should I consider purchasing data insurance or a cyber policy?

All business sizes from local barbers to large accountancy firms have data that could be compromised, and if this happens it could prove very costly. Cyber incidents are on the rise and a breach of your data can be expensive to rectify. By choosing to buy cover, you can maximise the security of your business while also taking responsible measures in terms of your data liability. No organisation is immune from the potentially devastating financial impacts of a cyber loss.

What sort of issues could I expect from a cyberattack that I could claim for?

You could expect to claim in the event that the systems that you use have been shut down, or your network has been breached. You could also potentially claim as a result of lost data via hardware e.g. your laptop, server or the devices your teams use to work remotely. Malicious use of your business data could also be claimed for.

Generally, through a cyber policy you could be covered for:

- Legal and defence expenses
- Coverage for PCI DSS fines.
- Extra expenses protection
- Theft of monies or securities digitally
- Third-party coverage for a privacy breach or data event
- Breach notifications
- Breach mitigation
- Data restoration
- Business income
- Coverage for regulatory fines
- GDPR costs incurred to the business

Protect your digital assets with cyber insurance

What is cyber business interruption?

This specific form of Business Interruption Insurance means that if your business has to close or cease trading temporarily as a result of a cyberattack, you can claim for loss of income. This is usually excluded from traditional insurance policies, so it is worth considering it even if you already have something like General Liability or Professional Indemnity.

What is PII?

PII stands for Personal Identifiable Information. The volume that is stored on your IT network could influence the cost of your premium, as more records means a higher risk.

It can include:

- Name
- Gender
- Address
- Email address
- Telephone number
- Etc.

let's **talk**

Have a more specific question or ready to enquire about cover?

Get in touch with us today on
0161 438 0000 or visit hinecyber.com

Hine®
CHARTERED INSURANCE BROKERS