PROTECT
COMMERCIAL INSURANCE

protectcommercial.co.uk

2021 CYBER SECURITY

BREACHES SURVEY

CYBER-SECURITY

THE RISK THAT KEEPS EVOLVING

The use of technology in daily operations continues to grow within organisations across sectors. The vast majority of businesses and charities already depended on at least one type of digital service, such as an online bank account, email, social media, e-commerce or electronic data storage.

While workplace technology can certainly provide a wide range of benefits to organisations, the risks that come with greater implementation are significant. In the past year, **39 percent of businesses** and **26 percent of charities** have experienced a data breach or cyber-attack. Furthermore, the consequences of these attacks are severe. Lost or stolen data, business interruption, costly non-compliance fines under the General Data Protection Regulation (GDPR) and reputational damage often accompany a data breach.

There are many different types of cyber-attack methods that hackers may utilise. Among the businesses and charities that experienced a cyber-attack within the past 12 months, 83 and 79 percent respectively reported falling victim to phishing attacks. The second-most common type of cyber-incident was impersonation, which 27 percent of businesses and 23 percent of charities experienced. These patterns generally remained consistent with trends in previous years.

While many organisations are taking steps to prevent the growing risk of cyber-attacks from wreaking havoc within their workplace, it's worth noting that 2021 saw a slight dip in the rate of organisations that prioritise cyber-security. **77 percent of businesses** and **68 percent of charities** now rate cyber-security as a high priority. This represents a slight decrease for both groups compared with percentages of 80 and 74, respectively, in 2020.

It's worth noting that the coronavirus pandemic has also had an impact on cyber-security. COVID-19 forced many organisations to improvise and expand their use of technology to accommodate remote work arrangements. Even though the conditions surrounding COVID-19 may now make it possible for workers to return to a traditional work environment, remote work is still expected to continue in many cases.

Remote workers may be seen as easier targets for cyber-criminals, but many organisations have not yet taken the necessary steps to protect themselves from these new or enhanced cyber-threats. In the past 12 months, only 35 percent of businesses deployed security monitoring tools compared with 40 per cent in the preceding year. Similarly, only 32 percent utilised any form of user monitoring compared with 38 percent previously. Furthermore, the percentage of both businesses and charities that have up-to-date malware protection has decreased from 88 to 83 percent and 78 to 69 percent, respectively. With these results in mind, Protect Commercial is proud to present our summary of the 2021 Cyber Security Breaches Survey, commissioned by the Department for Digital, Culture, Media & Sport as part of the National Cyber Security Programme.

As you read through these statistics, consider what you can do to bolster your business' or charity's cyber-security practices and GDPR compliance efforts. Don't miss out on the expansive opportunities of utilising digital services or resign your organisation to cyber-attacks because you failed to value cybersecurity.

Organisations can protect themselves and ensure digital success with cyber-risk management guidance and insurance solutions, available by contacting us today.

INCIDENCE AND IMPACT OF BREACHES

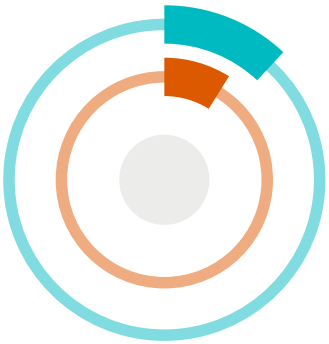
This section summarises how many businesses and charities have experienced breaches in the past year as well as the impact of those breaches. Specifically, it visually quantifies how many organisations have experienced a breach, the most disruptive forms of breaches and the most common negative impacts that accompanied a breach.

EXPERIENCE OF BREACHES:

39% of businesses and **26%** of charities experienced a breach in the past 12 months. Of these breaches:

23% of businesses and **24%** of charities needed new measures to prevent a future attack.

19% of businesses and **25%** of charities took up staff time dealing with the breach or attack.

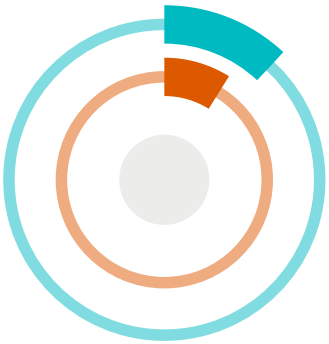


12% of businesses and **9%** of charities had to stop staff from carrying out their daily work.

Frequency of breaches in the last 12 months broken down:

23% of businesses and **24%** of charities needed new measures to prevent a future attack.

19% of businesses and **25%** of charities took up staff time dealing with the breach or attack.



12% of businesses and **9%** of charities had to stop staff from carrying out their daily work.

THE MOST DISRUPTIVE BREACHES:

Most disruptive forms of cyber-attack among organisations that reported more than one kind of attack in the past 12 months:

Phishing Attacks

(**67%** of businesses & **58%** of charities)

Others Impersonating The Organisation In Emails Or Online

(**11%** of businesses & **13%** of charities)

Viruses, Spyware, Malware Or Ransomware

(**7%** and businesses & **14%** of charities)

IMPACT OF BREACHES:

21% of businesses and **18%** of charities that experienced a breach or attack reported suffering negative outcomes, such as:

- **Temporary loss of access to files or networks**
- **Website or online services taken down or made slower**
- **Software or systems corrupted or damaged**
- **Money Stolen**

DEALING WITH BREACHES

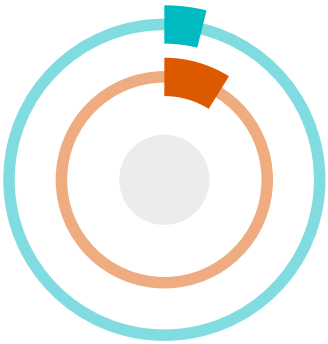
This section displays the numbers behind how organisations handled breaches in the past 12 months. Specifically, this section visually represents how long organisations took to recover from a breach, the average costs of a disruptive data breach and action taken by organisations following a cyber-attack.

TIME TAKEN TO RECOVER FROM BREACHES:

Average amount of time organisations spent dealing with their most disruptive breach in the last 12 months:

No time at all (**71%** of businesses and **67%** of charities)

24 hours or less (**18%** of businesses and **19%** of charities)



1-7 days (**4%** of businesses and **9%** of charities)

FINANCIAL COST OF BREACHES:

Average amount of time organisations spent dealing with their most disruptive breach in the last 12 months:

Businesses Overall: £2,670

Small Businesses: £2,600

Medium And Large Businesses: £3,930

Charities Overall: £2,110

The cost breakdown of businesses' most disruptive breaches in the past 12 months:

Average short-term direct cost: **£398**

Average staff time cost: **£740**

Average indirect cost: **£654**

Average estimated long-term cost: **£861**

UNDERSTANDING RESPONDING TO THE BREACH:

66% of businesses and **59%** of charities have at least some degree of cyberincident response procedures in place. The most common procedures include:

Attempting to identify the source of the incident

Debriefing to log any lessons learned

Assigning roles and responsibilities to specific individuals

Only **29%** of businesses and **23%** of charities reported their most disruptive breach to an external body other than their cyber-security provider.

Only **36%** of businesses and **46%** of charities formally log cyber-incidents.

In response to experiencing a breach, **62%** of businesses and **69%** of charities have taken steps to protect their organisation from future attacks. These efforts include:

Additional staff training or communications

Installed, changed or updated antivirus or anti-malware software

Changed or updated firewall or system configurations

APPROACHING CYBER SECURITY

This section provides information on what actions organisations have taken to bolster their cyber-security efforts. At a glance, this section identifies common cyber-security controls and policies organisations implemented, staff involvement related to cyber-security, how many organisations have followed government cyber-security initiatives, cyber-insurance trends and cyber-security documentation practices.

CYBER-SECURITY CONTROLS AND POLICIES

Organisations have implemented many different controls to bolster their cyber-security. The most common controls used include:

Having up-to-date malware protection

Restricting IT admin and access rights to specific users

Backing up data securely using a cloud service

Using firewalls that cover the entire IT network, as well as individual devices

Enforcing a password policy that ensures that users select strong passwords

33% of businesses and **36%** of charities have a formal policy or policies covering cyber-security risks. Common features of cybersecurity policies include:

- **How data is supposed to be stored**
- **What staff are permitted to do on their organisation's IT devices**
- **How remote or mobile working affects cyber-security**
- **What can be stored on removable devices, such as USB sticks**

Fewer organisations have conducted recent reviews of their cyber-security policies than in past years.

42% of businesses and **40%** of charities have not reviewed their cyber-security policies within the last six months.

14% of businesses and **20%** of charities have not reviewed their policies in the last year.

RECOGNISING SUPPLIER RISKS

Only **12%** of businesses and **8%** of charities have formally reviewed the potential cyber-security risks presented by their immediate supply chains.

Only **5%** of businesses and **4%** of charities have included their wider supply chains in such a review.

UNDERSTANDING GOVERNMENT INITIATIVES

50% of businesses and **45%** of charities have implemented at least five of the government's ***'10 Steps to Cyber-security.'*** This represents a **19%** drop for businesses and an **18%** decrease for charities compared to 2020 responses.

Only **4%** of both businesses and charities have implemented all 10 steps. These figures also decreased from **12%** and **14%**, respectively, last year.

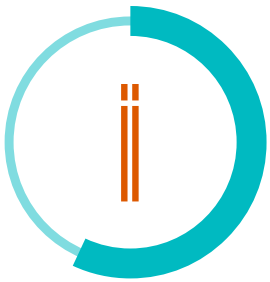
APPROACHING CYBER SECURITY CONT.

CYBER-INSURANCE

***43%** of businesses and **29%** of charities are insured against cyber-risks in some way.*

Cyber-insurance cover is more prevalent in certain industries, such as:

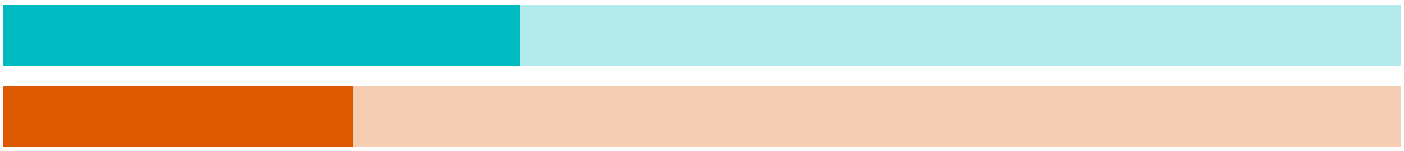
***60%** of organisations in the finance and insurance sector have cover*



***57%** of organisations in the information and communications sector have cover*

***53%** of organisations in the health, social care and social work sector have cover*

***53%** of organisations in the professional, scientific and technical sector have cover*



***37%** of businesses and **25%** of charities have cyber-security cover as part of a wide insurance policy.*

Only ***6%** of businesses and **4%** of charities have a specific cyber-insurance policy in place.*

DOCUMENTING CYBER-SECURITY

***Approximately half of both businesses and charities** have taken action to identify and document cyber-security risks in the past 12 months. Top actions include:*

Using specific tools designed for security monitoring

Conducting risk assessments related to cyber-security threats

Testing staff, such as with mock phishing exercises

Carrying out a cyber-security vulnerability audit

THE IMPORTANCE OF CYBER-SECURITY

TOP REASONS TO INVEST IN CYBER-SECURITY

Protect customer and consumer data.

Protect trade secrets, intellectual property and other assets.

Prevent fraud or theft.

Promote business continuity.

Protect the organisation's reputation.

Comply with data protection laws.

Protect against viruses.

Protect remote employees.

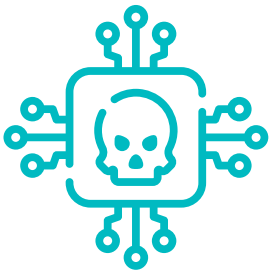
INVESTING IN CYBER-INSURANCE

WHY YOU NEED CYBER-INSURANCE

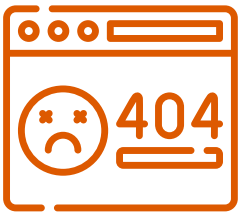
Government research suggests that cyber-insurance provides solutions for the following range of cyber-risks:

Privacy events.

Network security liability.



Cyber-crime.



Network business interruption.

Physical asset damage.

Reputational damage.

WE'RE HERE TO HELP

If you require any further information that is not covered in this document or simply wish to discuss any issues in more detail, please contact us on ***02921 677140*** or ***info@protectcommercial.co.uk***

PROTECT
COMMERCIAL INSURANCE

PROKNOW
INDUSTRY ACADEMY SERIES

2021 CYBER SECURITY BREACHES SURVEY

WWW.PROTECTCOMMERCIAL.CO.UK

If you require any further information that is not covered in this document or simply wish to discuss any issues in more detail, please contact us on 02921 677140 or info@protectcommercial.co.uk

Protect Commercial Insurance is a trading style of Protect Commercial Insurance Solutions Limited.
Registered in England & Wales No. 08365670

Registered Office: 33-35 West Bute Street, Cardiff, CF10 5LH.
Protect Commercial Insurance Solutions Limited is authorised and regulated by the Financial Conduct Authority