2024

Cyber-security Breaches Survey

philip gibbs insurance brokers

Table of Contents

Introduction

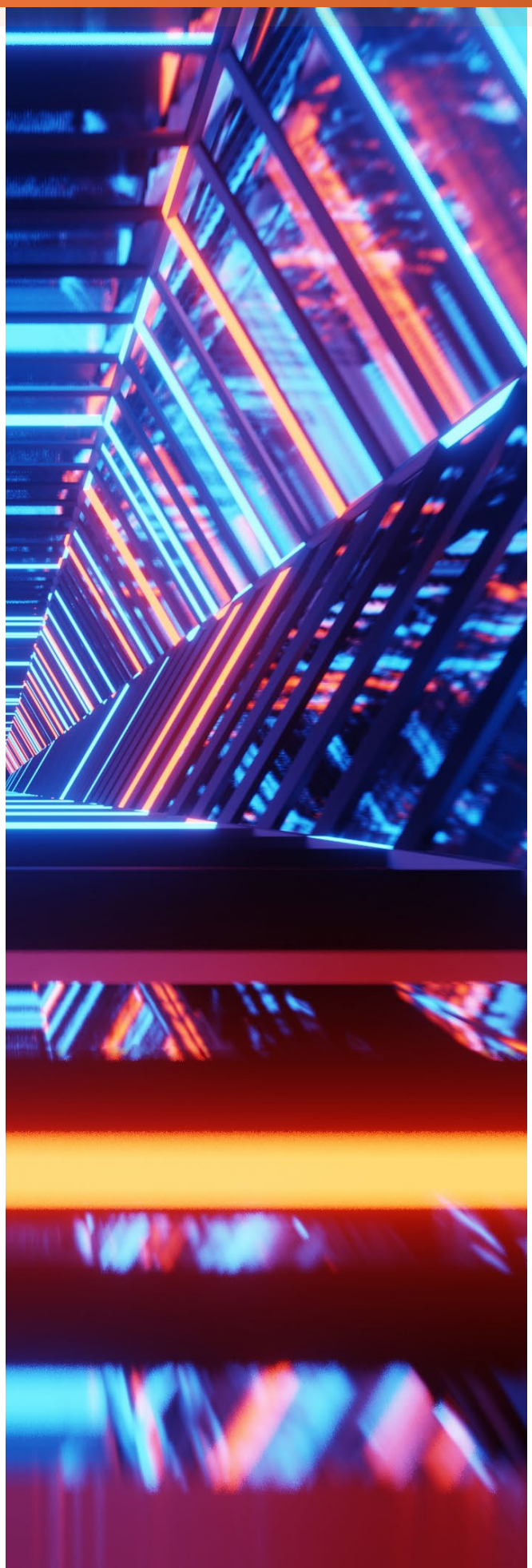
Year after year, cyber-security threats evolve at a rapid pace, and last year was no different. Geopolitical unrest continued in 2023, intensifying state-sponsored attacks, and artificial intelligence (AI) surged in popularity, providing another avenue for cyber-criminals to attack organisations. Consequently, staying abreast of the current trends in the cyber-landscape is imperative for organisations of all types and sizes.

The following report summarises data from the Cyber Security Breaches Survey 2024, commissioned by the Department for Science, Technology and Innovation as part of the National Cyber Security Programme. The figures within the survey illuminate areas where organisations could improve their cyber-security efforts.

As you read through the information, consider how your organisation could bolster its cyber-defences. Specifically, analyse trends, scrutinise cyber-security guidance and leverage best practices to improve risk mitigation efforts.

Contact us today for further cyber-risk management and insurance solutions.

Please refer to the glossary to see how the government defines organisations of various sizes.



Overview of Findings

Cyber-security Breaches Remain a Constant Threat

As cyber-criminals leverage evolving technology—especially generative AI—to develop new tactics to launch sophisticated attacks, cyber-security breaches are a pressing concern for organisations of all types and sizes. Although AI and other technology tools can help organisations achieve efficiencies and growth, employers may be exposed in unforeseen ways. Specifically, threat actors can leverage AI tools for nefarious purposes in several ways, including expediting credential cracking, creating and distributing malware, and deploying social engineering scams. This is especially true as technology becomes ingrained into most aspects of business operations.

In the past year, half (**50%**) of businesses and almost a third (**32%**) of charities experienced some form of cyber-security breach or attack. Segmented by size, this figure was even higher for medium-sized businesses (**70%**), large businesses (**74%**) and high-income charities (**66%**). What's more, among businesses experiencing breaches, **18%** experienced one per week, up from **11%** in last year's survey.

Regarding cyber-crime tactics, phishing continues to be the most common method. In fact, **84%** of businesses and **83%** of charities that fell victim to cyber-attacks were breached via phishing. Technological advancements have made phishing attacks more sophisticated. For instance, scams like business email compromise attacks are becoming increasingly difficult to detect. In these attacks, threat actors often leverage deepfake technology to impersonate a seemingly legitimate source (eg a CEO) via email, convincing the recipient to transfer money or reveal sensitive data.

The government reported that the cost of the single most disruptive breach per organisation averaged £1,205 in this year's survey, rising to £10,830 for medium and larger businesses, the latter figure more than double the £4,960 recorded in last year's survey. It's not just the cost of cyber-breaches impacting organisations; more than 1 in 10 (**13%**) businesses that identified a breach experienced a disruptive outcome, such as a temporary loss of networks and files, website downtime or compromised accounts.

With these findings in mind, it's vital that organisations across sectors implement a range of cyber-hygiene measures to lessen exposures. Encouragingly, both businesses and charities are now more likely to have a formal cyber-security strategy in place, the survey found. There was a significant increase for medium businesses (up from **49%** in 2023 to **58%** in 2024) and charities (up from **36%** to **47%**). Furthermore, more than half (**51%**) of businesses and **40%** of charities carried out some kind of risk mitigation activities, such as employing security monitoring tools, implementing penetration testing or performing mock phishing exercises.

While this upward trend is encouraging, there is still room for improvement with cyber-security measures, particularly pertaining to supply chain risks. Just **11%** of businesses have reviewed the cyber-security risks posed by their immediate supply chains, and only **6%** have included their wider supply chains. Considering that hundreds of UK firms were impacted after a third-party fire transfer system called MOVEit was hacked in 2023, taking steps to formally address the risks posed by third parties is prudent for organisations in 2024.

Continue reading for more insights into the current cyber-security landscape.

Incidence and Impact of Cyber-incidents

This section summarises the data of businesses and charities that have experienced breaches or attacks in the past year and the impact of those events. It visually quantifies how many organisations have experienced a cyber-incident, which types of incidents were disruptive and the most common negative impacts that accompanied them.

Experience of Cyber-incidents

50% of businesses and **32%** of charities reported experiencing a cyber-breach or attack in the past 12 months. Among these organisations:

14% of businesses and **21%** of charities adopted new measures to prevent future attacks.

14% of businesses and **25%** of charities needed additional staff time dealing with the breach or attack.

7% of businesses and **7%** of charities stopped staff from carrying out their daily work due to the breach or attack.

Here is the frequency of breaches in the last 12 months broken down:

Among businesses that experienced a breach, **20%** experienced just one, **24%** experienced fewer than one per month, **21%** experienced one per month, **18%** experienced one per week, up from **11%** in the 2023 survey. **14%** experienced one or more per day.

Among charities that experienced a breach, **22%** experienced just one, **31%** experienced fewer than one per month, **26%** experienced one per month, **10%** experienced one per week and **10%** experienced one or more per day.

The Most Disruptive Cyber-incidents

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

Phishing attacks
(**61%** of businesses and **56%** of charities)

Others impersonating the organisation in emails or online
(**16%** of businesses and **22%** of charities)

Takeovers or attempted takeovers of website, social media or email accounts
(**4%** of businesses and **4%** of charities)

Impact of Breaches

13% of businesses and **12%** of charities that experienced a breach or attack reported suffering negative outcomes, such as:

Website or online services taken down or made slower
(4% of businesses and 4% of charities)

Temporary loss of access to files or networks
(4% of businesses and 4% of charities)

Money stolen
(3% of businesses and 2% of charities)

Dealing with Cyber-incidents

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

Time Taken to Recover From a Cyber-incident

The average amount of time organisations took to get operations back to normal when dealing with their most disruptive breach in the last 12 months was as follows:

24 hours or less (**92%** of businesses and **91%** of charities):
No time at all (**79%** of businesses and **77%** of charities),
Less than a day (**13%** of businesses and **14%** of charities)

A week or less (**5%** of businesses and **6%** of charities)

Financial Costs of Cyber-incidents

The average total costs (ie short- and long-term costs, both direct and indirect) of the most disruptive breach or attack in the past 12 months among all organisations that reported a cyber-incident were:

Businesses overall: £1,205

Medium and large businesses: £10,830

Charities overall: £460

The average total costs of the most disruptive breach or attack in the past 12 months among organisations that reported an outcome to their cyber-incidents were:

Businesses overall: **£6,940**

Micro- and small businesses: **£4,590**

Medium and large businesses: **£40,400**

Charities overall: **£1,850**

Understanding and Responding to the Cyber-incident

Only **22%** of businesses and **19%** of charities had a formal cyber-incident response plan. Other common response measures were:

Informing senior management (**77%** of businesses and **81%** of charities)

Keeping an internal record of the incident (**54%** of businesses and **68%** of charities)

Assessing the scale and impact of the incident (**53%** of businesses and **63%** of charities)

Informing cyber-insurance providers (**50%** of businesses and **54%** of charities)

Debriefing to record lessons learnt from the incident (**50%** of businesses and **63%** of charities)

Attempting to identify the source of the incident (**45%** of businesses and **46%** of charities)

Informing a regulator of the incident when required (**44%** of businesses and **56%** of charities)

Only **34%** of businesses and **37%** of charities reported their most disruptive breach outside of their organisation. When removing organisations who only reported breaches to their external cyber-security or IT providers, this figure dropped; **25%** of businesses and **29%** of charities reported their most disruptive breach externally.

In response to experiencing a breach, **59%** of businesses and **70%** of charities took steps to protect their organisations from future attacks. These efforts included:

Enhancing staff training or communications

Installing, changing or updating antivirus or anti-malware software

Changing or updating firewall or system configurations

Approaching Cyber-security

This section provides information on the actions organisations have taken to bolster their cyber-security efforts in the last 12 months.

Cyber-security controls and policies

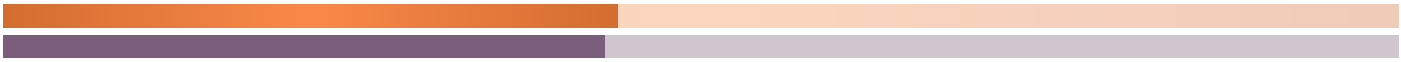
The most common controls organisations implemented to bolster their cyber-security included:

- Using up-to-date malware protection
- Using firewalls that cover the entire IT network, as well as individual devices
- Restricting IT admin and access rights to specific users
- Enforcing a password policy that ensures that users select strong passwords
- Backing up data securely using a cloud service

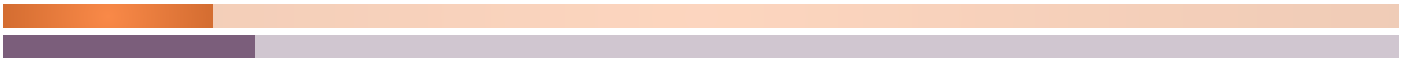
33% of businesses and **32%** of charities had a formal policy or policies covering cyber-security risks. Common concerns cyber-security policies address were:

- The process by which data is supposed to be stored
- The activities staff are permitted to do on their organisation's IT devices
- The ways in which remote or mobile working affects cyber-security
- The use of network-connected devices
- Use of cloud computing
- The items that can be stored on removable devices, such as USB sticks
- Use of personally owned devices for business activities

Of the organisations that have formal policies covering cyber-security risks:

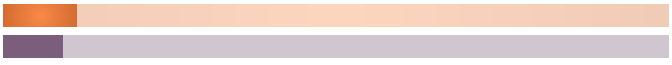


44% of businesses and **43%** of charities reviewed their cyber-security policies within the last six months. This figure is largely similar to the last few years for businesses but still below the 52% figure recorded in the 2020 survey, showing there is room for improvement. Encouragingly, the figure for charities is 9% higher than 2023's survey.

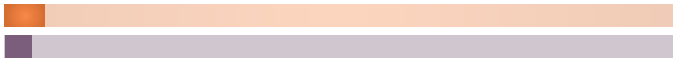


15% of businesses and **18%** of charities have not created, updated or reviewed their policies in over a year.

Recognising Cyber-risks



Only **11%** of businesses and **9%** of charities formally reviewed the potential cyber-security risks presented by their immediate supply chains.



Only **6%** of businesses and **4%** of charities included their wider supply chains in such reviews.

Approaching Cyber-security (cont.)

Understanding Government Initiatives

39% of businesses and **32%** of charities implemented at least five of the government's "10 Steps to Cyber Security," a marginal improvement on last year's figures.

Only **3%** of all businesses and charities implemented all 10 steps. Medium and large businesses fared better, with **14%** and **27%** enacting all 10 steps.

Cyber-insurance

43% of businesses and **34%** of charities were insured against cyber-risks in some way.

35% of businesses and **29%** of charities had cyber-security cover as part of a wider insurance policy.

Only **8%** of businesses and **5%** of charities had a specific cyber-insurance policy in place.

Documenting Cyber-security

51% of businesses and **40%** of charities took action to identify and document cyber-security risks in the past 12 months, unchanged from last year. Top actions included:

- **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

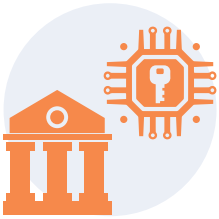
Protect customer and consumer data.

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 computer viruses.

Protect remote employees.

Glossary

Organisation sizes

The following are definitions used by the government to describe organisations of various sizes.

Micro-business	Businesses with one to nine employees
Small business	Businesses with 10 to 49 employees
Medium business	Businesses with 50 to 249 employees
Large business	Businesses with 250 or more employees
Low-income charity	Charities with an income of less than £100,000
High-income charity	Charities with an income of £500,000 or more

---

Data Sources and Reliability

This year's data was gleaned from the responses of UK businesses over 12 months. Main survey interviews took place between September 2023 and January 2024, and qualitative follow-up interviews took place in December 2023 and January 2024.

Please note that the data wasn't based on the entire population of UK businesses or charities but rather on weighted samples. As such, percentage results are subject to margins of error. Additionally, due to changes to some questions, readers are advised to be careful when comparing the 2023 and 2024 datasets. Visit the government website for more information.