2023 CYBER-SECURITY BREACHES SURVEY

riskhub
the business resilience people

TABLE OF CONTENTS

INTRODUCTION

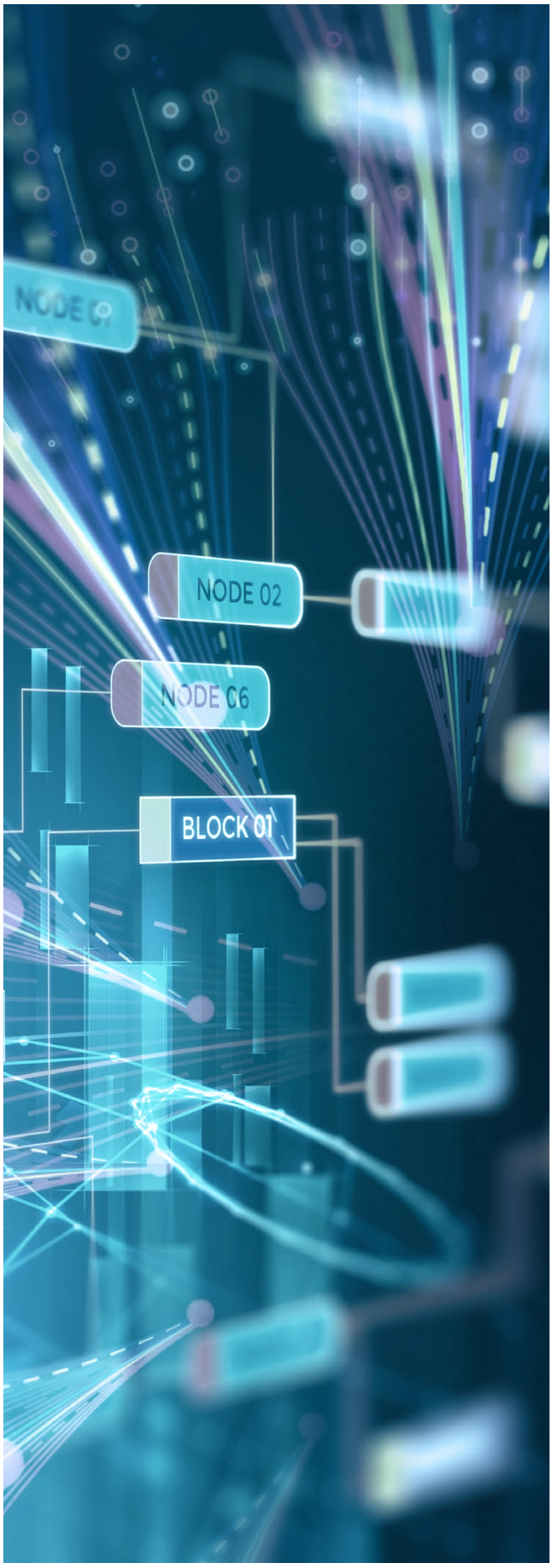
Cyber-security risks continue to evolve each year alongside new advancements. The development of artificial intelligence (AI) and the rapid growth of Internet of Things devices have increased the ways that cyber-criminals can attack.

The following report summarises data from the Cyber Security Breaches Survey 2023, commissioned by the Department for Science, Technology and Innovation as part of the National Cyber Security Programme. Ultimately, the figures within the survey illuminate areas where organisations of all sizes could improve their cyber-security efforts.

As you read through the figures, 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 TRENDS CONTINUE TO EVOLVE

Innovative technology can improve how employees work and increase profitability; however, it may also leave organisations exposed in unforeseen ways. This is especially true as new technology becomes more entwined with daily operations. Indeed, the consequences of a cyber-attack may involve service disruption, loss of file or network access, and corrupted software, among many others. What's more, these attacks aren't always one-off events.

In the last year, among organisations that experienced cyber-breaches or attacks, **40%** of businesses and **38%** of charities reported that such incidents happened once a month; **21%** of businesses and **19%** of charities reported one cyber-incident per week.

Overall, **32%** of UK businesses and **24%** of UK charities experienced a cyber-security breach or attack in the past 12 months. Segmented by size, the rate is notably higher for medium businesses (**59%**), large businesses (**69%**) and high-income charities (**56%**); among these organisations, the year-on-year rates of cyber-incidents were approximately unchanged. Yet, when factoring in organisations of all sizes, reported cyber-incidents actually decreased year on year—down **7%** and **6%** for businesses and charities, respectively.

The survey revealed the general decrease was driven primarily by smaller organisations. Amid an uncertain economic climate, it may be that these companies struggled to stretch scant resources to meet all business challenges. Consequently, cyber-security and logging of breaches fell by the wayside. Indeed, the proportion of micro-businesses considering cyber-security as a "high priority" has decreased from **80%** in 2022 to **68%** this year. In contrast, medium businesses, large businesses and high-income charities continue to treat cyber-security more seriously, which makes sense considering they are still prime targets for cyber-criminals.

Regarding tactics used for cyber-attacks, the survey findings are similar to 2022's data. Phishing was reported as the most disruptive attack method by **59%** of businesses and **64%** of charities. Additionally, impersonation was the root cause of breaches within **31%** of businesses and **29%** of charities, an uplift from the **27%** and **26%** reported in the Cyber Security Breaches Survey 2022. Heightened AI tool popularity could be the cause of this increase, with chatbots and voice-cloning tools now making it easier for hackers to fool victims.

Fortunately, the majority of businesses and charities have a broad range of basic controls in place to protect themselves from cyber-attacks. In fact, **76%** of businesses and **63%** of charities have up-to-date malware; **70%** and **55%** enforce strong password policies; and **70%** and **50%** back up data via secure cloud services. Taking this further, **66%** of businesses and **68%** of charities have implemented specific steps in response to a breach to protect themselves from future attacks—up from **62%** and **57%**, respectively, the previous year. Actions include updating firewall or system configurations and revising staff training. While this upward trend is encouraging, there is still room for improvement; cyber-security measures currently underutilised by organisations include two-factor authentication, user activity monitoring and virtual private network use.

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 throughout the past year and the impact of those events. Specifically, 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

32% of businesses and **24%** of charities reported experiencing a cyber-breach or attack in the past 12 months. Among these organisations:

21% of businesses and **23%** of charities adopted new measures to prevent future attacks.

23% of businesses and **26%** of charities needed additional staff time dealing with the breach or attack.

11% of businesses and **11%** of charities stopped staff from carrying out their daily work.

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

Among businesses that experienced a breach: **28%** experienced just one, **29%** experienced fewer than one per month, **19%** experienced one per month, **11%** experienced one per week, and **11%** experienced one or more per day.

Among charities that experienced a breach: **29%** experienced just one, **28%** experienced fewer than one per month, **19%** experienced one per month, **11%** experienced one per week, and **8%** 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 (excluding those that only identified phishing attacks) were:

Phishing attacks
(**59%** of businesses and **64%** of charities)

Others impersonating the organisation in emails or online
(**35%** of businesses and **41%** of charities)

Hacking or attempted hacking of online bank accounts
(**15%** of businesses and **9%** of charities)

IMPACT OF BREACHES

24% of businesses and **18%** of charities that experienced a breach or attack reported suffering negative outcomes, such as:

Website or online services taken down or made slower
(8% of businesses and 7% of charities)

Temporary loss of access to files or networks
(8% of businesses and 6% of charities)

Money stolen
(7% of businesses and 2% of charities)

Software or systems corrupted or damaged
(5% of businesses and 3% 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 spent dealing with their most disruptive breach in the last 12 months was as follows:

No time at all (**70%** of businesses and **72%** of charities)

Within a day (**19%** of businesses and **15%** of charities)

Within a week (**8%** of businesses and **9%** 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: £1,100**
- **Microbusinesses and small businesses: £870**
- **Medium and large businesses: £4,960**
- **Charities overall: £530**

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: **£3,770** | Microbusinesses: **£2,950** | Medium and large businesses: **£15,800** | Charities overall: **£2,310**

UNDERSTANDING AND RESPONDING TO THE CYBER-INCIDENT

Only **21%** of businesses and **16%** of charities have a formal cyber-incident response plan. Other common response measures include:

- **Informing senior management**
- **Informing cyber-insurance providers**
- **Keeping an internal record of the incident**
- **Assessing the scale and impact of the incident**
- **Debriefing to record lessons learnt from the incident**
- **Informing a regulator of the incident when required**

Only **38%** of businesses and charities reported their most disruptive breach outside of their organisation, and even then, it's often only reported to their cyber-security providers. This indicates that cyber-threats—and their severity—may be underreported and greater than currently known.

In response to experiencing a breach, **66%** of businesses and **68%** 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 in the last 12 months.

CYBER-SECURITY CONTROLS AND POLICIES

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

- **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**

29% of businesses and **35%** of charities have a formal policy or policies covering cyber-security risks. Common concerns cyber-security policies address include:

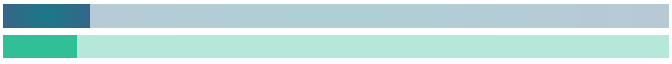
- **The process by which data is supposed to be stored**
- **The activities staff are permitted to do on their organisation's IT devices**
- **The ways in which remote or mobile working affects cyber-security**
- **The items that can be stored on removable devices, such as USB sticks**
- **Use of cloud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

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

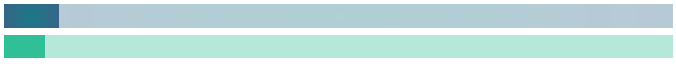
45% of businesses and **34%** of charities have reviewed their cyber-security policies within the last six months. This figure is largely similar to the last two years but still below the **52%** figure recorded in the 2020 survey, showing there is room for improvement.

12% of businesses and **25%** of charities have not created, updated or reviewed their policies in over a year.

RECOGNISING CYBER-RISKS



Only **13%** of businesses and **11%** of charities have formally reviewed the potential cyber-security risks presented by their immediate supply chains.



Only **8%** of businesses and **6%** of charities have included their wider supply chains in such a review.

UNDERSTANDING GOVERNMENT INITIATIVES

37% of businesses and **30%** of charities have implemented at least five of the government's "10 Steps to Cyber Security." This represents a **12%** drop for businesses and **10%** drop for charities compared with last year's responses.

Only a combined **2%** of all businesses and charities have implemented all 10 steps, half of last year's **4%** figure. Medium and large businesses fare better, with **7%** and **20%** enacting all 10 steps.

APPROACHING CYBER-SECURITY, CONT.

CYBER-INSURANCE

37% of businesses and **33%** of charities are insured against cyber-risks in some way.

Cyber-insurance cover is more prevalent in certain industries:

48% of businesses in the finance and insurance sectors have cover.

52% of businesses in the professional, scientific and technical sectors have cover.

30% of businesses and **25%** of charities have cyber-security cover as part of a wider insurance policy.

Only **7%** of businesses and **8%** of charities have a specific cyber-insurance policy in place, although this has increased by **2%** and **3%**, respectively, compared to last year's figures.

DOCUMENTING CYBER-SECURITY

51% of businesses and **40%** of charities have taken actions to identify and document cyber-security risks in the past 12 months. Compared with the 2022 figures, this represents a slight decrease for both businesses (**-3%**) and charities (**-1%**). 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 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
Very high-income charity	Charities with an income of £5 million or more