trowers & hamlins

—— trowers.com

# Cyber Security Breaches Survey 2024

## Insights from breaches to best practice

May 2024 ——

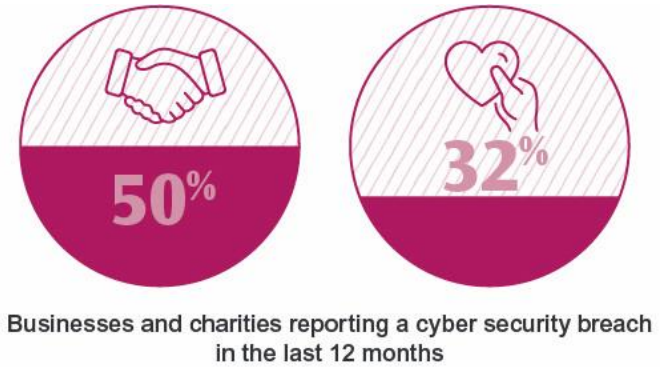
## Cyber Security Breaches Survey 2024

On 9 April 2024, the Department for Science, Innovation & Technology (the 'DSIT') published its annual Cyber Security Breaches Survey (the 'Survey'). The Survey delves into the policies, processes and approach to cyber security by businesses, charities and educational institutions. It highlights that cyber security breaches and attacks continue to be a common threat for organisations and looks at how they are adapting to these situations.

Cybersecurity remains an ever-present threat to organisations. There have been many high-profile cybersecurity incidents in the last year, affecting some of the world's biggest organisations. For example, there has been a number of notable cyber-attacks including, only last month a Serbian hacker accessed Space-Eyes, a firm that works exclusively for US government agencies, and has alleged to have accessed sensitive data, the British Library is still continuing to experience a technology outage as a result of the attack caused in October 2023, and just last week, it was announced the Ministry of Defence payroll system experienced a hacking attack, with 270,000 serving personnel had their details stolen.

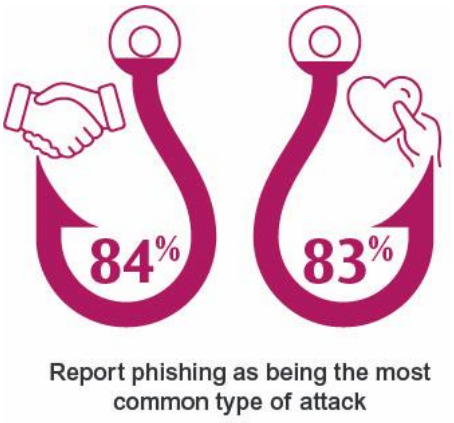
## Cybersecurity incidents

In the 12 months prior to the Survey, 50% of businesses and 32% of charities reported experiencing some kind of cyber security breach or attack. This is believed to affect 718,000 businesses and 65,000 charities each year.



Businesses and charities reporting a cyber security breach in the last 12 months

The most common type of attack was phishing (84% of businesses and 83% of charities), where staff receive fraudulent emails or are directed to fraudulent websites, followed by, albeit to a lesser extent, others impersonating organisations in emails or online (35% of businesses and 37% of charities), then viruses or other malware (17% of businesses and 14% of charities). Phishing attacks were often seen to be the most disruptive attack that an organisation faces however, most organisations were able to restore operations within 24 hours.





## Current protections in place by organisations

Despite the continued prevalence of cybersecurity attacks and breaches, a minority of organisations have an agreed process in place for incident response – only 22% of business and 19% of charities had formal incident response plans.


The Survey looked at "cyber hygiene" measures within organisations, such as using up to date malware protection and restricting admin rights. It was noted that the most common cyber threats are often unsophisticated, and therefore government guidance advises organisations to increase resilience by implementing these kinds of measures. The use of these cyber hygiene measures within businesses and charities has risen compared to 2023. For example, 75% of businesses now deploy network firewalls, compared to 66% last year. However, this is still a cause for concern to central government. In January 2024, the DSIT issued a 'Cyber Governance Code of Practice: call for views' with the intention to support directors to drive greater cyber resilience. A link to our article about the Cyber Code of Practice can be found here.

Further, the Survey asked businesses and charities about their risk management procedures. The results are that just under one third of businesses and just over one quarter of charities had undertaken a cyber security risk assessment in the last year, and this was more prevalent in medium and large businesses. When reviewing risks, only 11% of businesses and 9% of charities reviewed the risks posed by immediate suppliers. The Survey found that there was an increasing awareness of the cyber security risks posed by immediate suppliers in their supply chain but

many organisations, particularly smaller ones, had limited formal procedures in place to manage these risks.

Levels of board engagement and corporate governance approaches towards cyber security have remained stable compared to the 2023 survey. 75% of businesses and 63% of charities report that senior management see cyber security as a high priority, rising to 98% in large businesses. 30% of charities, 51% of medium businesses and 63% of large businesses have board members or trustees who are responsible for cyber security as part of their role. In interviews undertaken for the Survey, it was found that issues such as lack of knowledge, training and time prevented boards from engaging with cyber security.

Reasons preventing boards from engaging with cyber security

## Key takeaways from the Survey

Whilst it is clear that the importance of cybersecurity sits as a high priority on the agenda, the difficulties remain for boards in investing time and budget in order to increase their organisations' cyber resilience. Nonetheless there are several simple steps that every organisation can take to enhance their cybersecurity:

- **Make use of guidance:** the Survey highlights businesses seeking external guidance on cyber security has fallen since last year. In particular, the National Cyber Security Centre hosts a wealth of helpful guidance – such as Cyber Aware - NCSC.GOV.UK and 10 Steps to Cyber Security - NCSC.GOV.UK. Outsourcing to trusted legal and technical expert advisors will also ensure regulatory compliance and identify any potential vulnerabilities.

- **Enhance training and awareness:** phishing is the most prevalent and disruptive form of incident most organisations face. The Survey found that currently only around a fifth of all organisations provide training to staff. Ensuring that staff are sufficiently trained and are aware of the risks can help to mitigate them as staff will then know what to look out for and what they should do in an event of an attack.


- **Consider insurance options:** currently 43% of businesses and 34% of charities are insured against cyber security risks in some way, however this is mostly as part of a wider policy. Organisations seeking cyber insurance will likely find they must demonstrate that cyber risk is being mitigated and managed, failing which insurance may not be attainable, let alone cover breach costs or business interruption.
- **It's the little things:** having good cyber hygiene is often made up of small steps which will increase resilience, such as installing multi-factor authentication, making sure software is updated with the latest version and regular system back-ups.
- **Organisations should avoid informal response planning:** clear plans and processes in place responding to any cyber incidents that occur will reduce the risk of business disruption and result in quicker restoration of operations.
- **Think about your supply chain:** the saying goes that you are only as strong as your weakest link – the same goes for supply chains. Do you have security critical requirements in your contracts? Do you have any assurance on suppliers' cybersecurity infrastructure? There are a few processes all organisations need to consider with potential and existing suppliers to decrease risk to your organisation and customer base whilst maintaining trust and good communication with suppliers.

We work with clients proactively to mitigate risk, putting clients' cyber planning on the front foot; bringing knowledge, understanding and solutions no matter the client's market or size. Combining the legal excellence of Trowers' cyber team and award-winning cyber experts, CyberQ, CyberSecure 360 offers legal and technical cybersecurity advice tailored to clients' requirements – from assessing compliance with cyber policies, undertaking risk assessments through penetration testing and incident response planning to providing training and playing out war-room scenarios in real time. For more information or to discuss your cyber and fraud prevention needs please contact our specialist cyber and fraud team:

**Helen Briant**
**Partner**
Dispute Resolution and Litigation
+44 (0)121 214 8867
HBriant@trowers.com

**Charlotte Clayson**
**Partner**
Dispute Resolution and Litigation
+44 (0)20 7423 8087
CClayson@trowers.com

**Elizabeth Mulley**
**Managing Associate**
Dispute Resolution and Litigation
+44 (0)121 214 8864
EMulley@trowers.com

**Amy-Rose Hayden**
**Associate**
Dispute Resolution and Litigation
+44 (0)121 203 5672
AHayden@trowers.com