trowers & hamlins

—— trowers.com

Cyber Security Breaches Survey 2023

WHAT CAN WE LEARN FROM THE DATA?

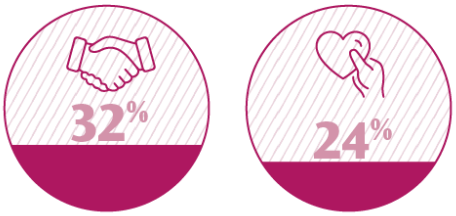
Cyber security breaches survey 2023

On 19 April 2023, the Department for Science Innovation and Technology published its annual Cyber Security Breaches Survey ('the Survey'), looking into the UK's cyber resilience across a range of businesses and charities.

The Survey provides a wealth of data that helps us to understand how common cyber attacks might be, how businesses and charities alike can be affected, how prepared we are to respond to such attacks, and how organisations are prioritising cyber resilience in the current economic and geo-political climate.

So how common are cyber security incidents?

The UK government highlights that cyber security breaches remain a common threat across a range of businesses and charities. Whilst 32% of businesses and 24% of charities reported cyber security breaches in the last 12 months, this is a decrease from last year's Survey. Despite the decrease, the statistics show that this is a significant and real-world issue affecting around 462,000 businesses and 48,000 registered charities over the last 12 months.



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

Of those organisations reporting cyber breaches, around 40% of businesses and 38% of charities report these incidents happening at least once a month, and 21% of businesses and 19% of charities reporting cyber incidents at least once a week.

% of businesses and charities reporting cyber breaches once a month and once a week

What part does the economy play in cyber risk?

It's difficult to know for certain what has caused the decline in the proportion of organisations reporting cyber security breaches over the last year, and whether this demonstrates a genuine change in the risk landscape. However, whilst the data shows a decline the Survey also suggests that this has been driven by a drop in reporting from smaller organisations: medium and large businesses and high-income charities are reporting cyber breaches at similar levels to the previous year.

The Survey shows a drop in the relative priority given to cyber issues by organisations over the last year, a drop from 82% to 71% of businesses considering cyber security to be a 'high priority' and a similar drop from 72% to 62% for charities.

However, much of the decrease can be attributed to the significant drop from 80% to 68% of micro-businesses considering it a 'high priority' this year. As well as the statistical data collected by the Survey, significant insight can be gained from the interviews undertaken with organisations, many of which have highlighted the difficulties they have in balancing cyber risk management against rising energy prices, inflation and an uncertain economic climate. It seems this has had a real impact on the ability of smaller organisations to monitor and log cyber incidents, which in turn has had an effect on reporting numbers.

What are the most common cyber threats?

The most common threat to organisations remains from phishing attacks, focussed on sending fraudulent emails to staff, or directing them to fraudulent websites. Of the UK organisations who had identified an attack, 79% reported threats arising from phishing scams, 31% from people impersonating organisations in emails or online, followed by 11% reporting threats from malware. These figures are considerably higher when looking at medium and large organisations in isolation, which are more likely to report these types of incidents.

How are organisations responding to cyber risk?

The UK government recommends that organisations put a range of 'cyber hygiene' measures in place, such as use of password policies, network firewalls and policies to quickly apply software security updates. However, the Survey data shows that deploying these measures has fallen since last year, and this represents a significant cyber hygiene challenge, particularly amongst micro businesses and SMEs.

Yet despite the strong message from the UK Government and the National Cyber Security Centre about the risk that supply chain vulnerabilities can cause - whether from threat actors using supply chains to gain access to an organisation's systems, to phishing attacks, viruses and malware originating from suppliers - very few organisations are taking steps to formally assess that risk. Just one in ten organisations are reviewing the risks presented in their immediate supply chain, with even fewer looking at the wider supply chain. The recent high profile cyber-attack on outsourcing group Capita, which holds more than £6.5 billion worth of public sector contracts, demonstrates the risks that supply chains can present to organisations, and the need to keep those risks under review through the contract life-cycle, from procurement through to contract management.

Actively review the risks presented in their immediate supply chain

But it is not just the technical side where engagement is dwindling. The organisational side also shows some concerning trends around dwindling engagement from board members on cyber issues, common reasons for this being a lack of understanding or interest, and SMEs briefing boards on an informal basis, or only in response to incidents arising. It seems that issues around limited training and education, which does not require a significant investment, but which is an integral part of cyber security, is not just limited to the Board. Figures in the Survey show that in the last 12 months, only 18% of businesses and 17% of charities have provided staff with formal training on cyber security risks. This is a clear area for organisations to manage their cyber risk efficiently and effectively, particularly in the face of economic uncertainty.

Turning to the ability of organisations to react promptly to cyber security breaches, the Survey shows that whilst large numbers of organisations said that they would take steps to respond to cyber incidents, very few actually had formal processes and procedures in place: only 21% of businesses and 16% of charities have incident response plans in place.

Businesses and charities having incident response plans in place

What's the impact?

The Survey estimates that across all UK businesses, there were around 2.39 million instances of cyber-crime and 49,000 incidents of related fraud over the last 12 months.

The true costs of cyber incidents are more than just a number and can lead to business interruption, lost trade, and the costs of internal investigations and disciplinary procedures. Investors are increasingly looking at cyber risks as a key metric in assessing value, and related ESG requirements.

As well as re-directing staff and resources to deal with breaches, cyber incidents affect staff morale, consumer confidence and reputation in ways that are hard to measure, but which cannot be underestimated in an uncertain economic climate.

Regulators such as the Information Commissioner's Office regularly fine organisations who haven’t got things right – the recent case of Interserve, which was fined £4.4m for its failures to

prevent a cyber-attack affecting 113, 000 individuals, is a case in point. Threatened legal action from individuals whose data has been affected and who want to seek compensation from the organisation is also increasingly becoming a standard response to cyber-attacks.

What should I take away from the Survey?

Cyber risk is here to stay. Despite the difficult economic environment, there are a number of steps that organisations of all sizes can take to effectively and efficiently manage the risks associated with cyber security incidents:

A whole organisation approach: no risk can be managed in isolation, and cyber risk is no different. Make sure that your internal or external IT teams are communicating with your risk teams, DPOs, procurement teams and the board to ensure that the true risks to the business are understood and managed.

Work with IT teams to assess internal safeguards and capabilities: managing cyber risk from the technical side does not need to be scary or expensive. Assess your current operating environment and take steps to implement solutions that are proportionate to your business risk and budget.

Reviewing policies, procedures and information governance to ensure regulatory compliance: Organisations should engage with industry standards such as Cyber Essentials to protect against the most common cyber threats such as phishing attacks. Small organisations should also use the Small Business Guide to improve cyber security practises. Larger organisations should use the Board Toolkit to get company executives to act on cyber resilience. Charities should follow the Small Charity guide to boost cyber security operations. Furthermore, organisation should keep their software and systems fully up to date to prevent hackers exploiting any weaknesses.

Formulating effective breach response plans: Organisations should avoid taking an informal approach to incident management and should adopt a formal business continuity plan with a focus on maintaining operations in response to a serious breach and encouraging a proactive approach to cyber risk management.

Training and awareness: People are a key asset in managing your cyber risk. The Survey highlights the importance of cyber security skills and training, to create engaging culture amongst staff around cyber security and enable organisations to practice good cyber hygiene.

Want to hear more? In our podcast, Charlotte Clayson and Liz Mulley provide top tips on how to prepare for a potential attack. Joined by guests Neil Belton, Director of Technology Risk and Paul Kelly, Head of Cyber Services at business advisory service, Azets. They discuss best practices, current cyber security trends and the crucial role staff within organisations play in preventing cyber-attacks. You can listen to it **here.**

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
Senior Associate
Dispute Resolution and Litigation
+44 (0)121 214 8864
EMulley@trowers.com