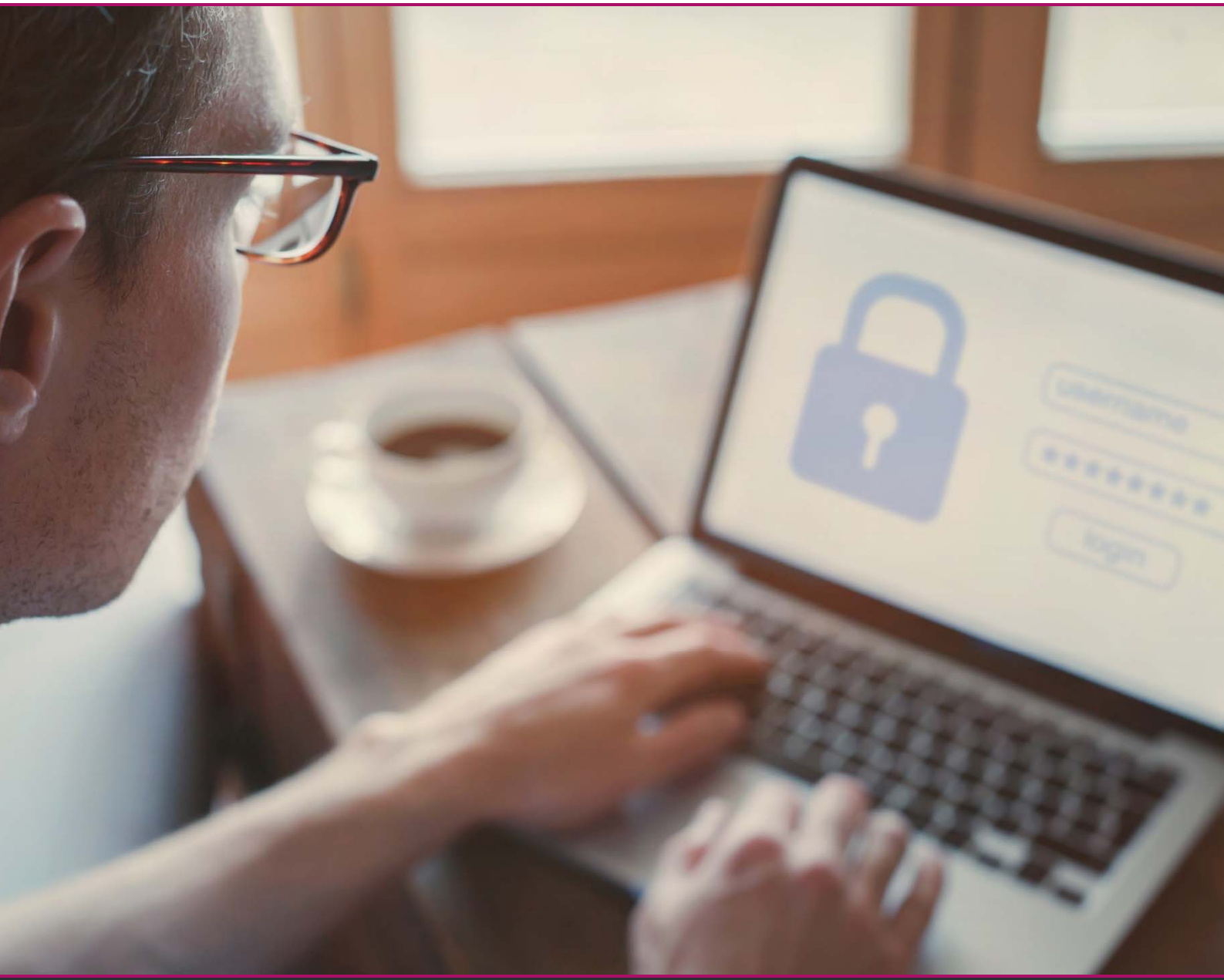
trowers & hamlins

—— trowers.com

Cyber Security Breaches Survey 2022

FINDINGS AND HOW TO PREVENT AN ATTACK



Cyber security breaches survey 2022

On 30 March 2022, the Department for Digital, Culture, Media and Sport (DCMS) published its annual Cyber Security Breaches Survey (the "Survey"). This is the UK's most influential research study regarding cyber resilience. The Survey explores the policies, processes, and approaches to cyber security for businesses, charities, and educational institutions. The Survey therefore highlights how organisations approach cyber security as well as how they adapt and react to an evolving threat landscape.

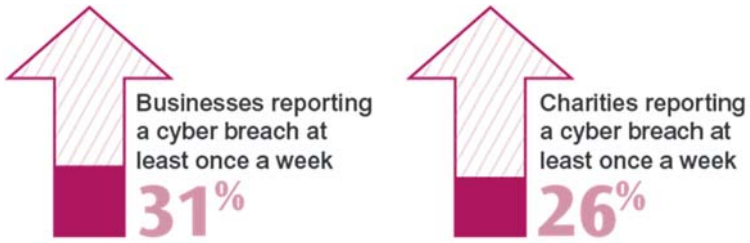
What does the Survey show?

The UK government is urging businesses and charities to strengthen their cybersecurity practices, as the Survey shows that the frequency of cyberattacks is increasing. Almost a third of charities (30%) and two in five businesses (39%) reported cybersecurity breaches or attacks in the last 12 months.

% charities reporting a cyber security breach in the last 12 months

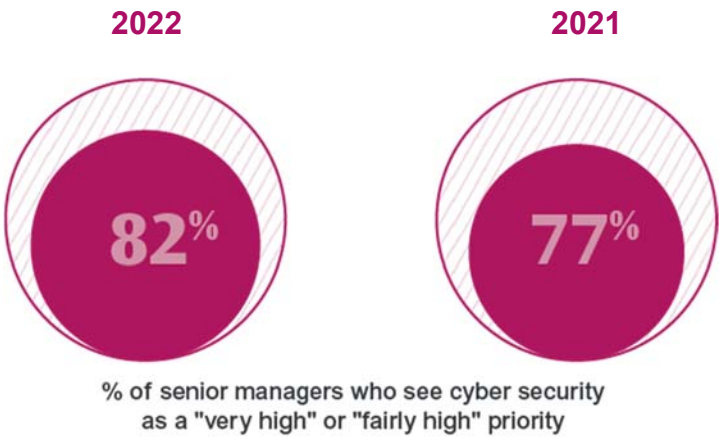
% businesses reporting a cyber security breach in the last 12 months

Whilst the number of businesses that experienced an attack or breach remained the same as in 2021, almost one in three businesses (31%) and a quarter (26%) of charities suffering attacks said that they now experience breaches or attacks at least once a week. The frequency of cyberattacks is, therefore, rising.



There has been a wave of high-profile attacks over the past year, in particular, the "Microsoft Exchange Hack" where hackers compromised Microsoft Exchange Outlook, giving them access to victims' entire server and network as well as emails and calendar invitations. As such, there is

no surprise that the Survey found, four out of five senior managers (82%) in UK businesses now see cyber security as a "very high" or "fairly high" priority, from 77% in 2021.



In terms of how cyberattacks are being carried out, the Survey found that of the 39% of UK businesses who identified an attack, the most common threat vector was phishing attempts (83%), with 21% identifying more sophisticated attack types such as a denial of service, malware, or ransomware attacks. The Survey found that organisations have been able to implement engaged culture around cyber security, understanding that staff vigilance is essential to protecting against phishing attacks.

83% Phishing attempt

21% Malware, denial of service or ransomware

The Survey found that organisations have been able to maintain good cyber hygiene, with most rules, policies and controls and risk mitigation techniques remaining steady compared to last year, despite continued challenges. For instance, more than four in five medium and large businesses have taken action for their cyber security in at least five areas detailed in the Government guidance: the 10 Steps to Cyber Security. This demonstrates that larger UK organisations have a good standard of cyber security, which is encouraging.

The Survey, however, found that 40% of businesses and almost a third of charities (32%) are using at least one managed service provider, but only 13% of businesses reviewed the risks posed by immediate suppliers, with organisations saying that cyber security was not an important factor in the procurement process. As such, the findings from this year's survey demonstrate that there is still a lot to be done to improve organisations' cyber hygiene. With such findings, it makes sense that the Government has identified supply chains as a big cyber risk to organisations and are focusing on this risk area as part of its National Cyber Strategy 2022.

How to prevent an attack?

The Survey serves as an important reminder for organisations to review and strengthen their cybersecurity practices, which can be done by implementing the following cost efficient steps:

Working with IT specialists to assess internal safeguards and capabilities: the Survey highlighted that despite cyber security being a high priority, there is a lack of technical knowhow expertise within organisations in respect of preventing cyber-crime. As such, companies should work with IT specialists to strengthen the awareness of strategic risks posed by their organisations.

Advising on strategies to minimise key commercial, financial, regulatory and legal risks: For instance, organisations should effectively negotiate a cyber security budget against other competing organisational priorities. Failing to consider a cyber security budget may mean that organisations take a reactive approach to cyber incidents as opposed to a proactive approach in limiting cyber risks.

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.

Advising on sector specific issues, best practice and formulating effective breach response plans: Organisations should avoid taking an informal approach to incident management and should adopt a formal business continuity plan. By adopting a formal business continuity plan, this means there is a focus on maintaining operations in response to serious breach and a proactive stance to cyber risk management.

Working closely with your teams to implement breach response plans to protect data and mitigate key business risks: the Survey highlights the importance of cyber security skills and training, which will give rise to an engaging culture amongst staff around cyber security and enable organisations to practice good cyber hygiene.

Take away

The true cost of a cyberattack is more than just a number. Penalties from regulators and damage to reputation can lead to business disruption, lost trade, management time and the costs of internal investigations and disciplinary procedures. As such, getting your cyber house in order has never been more important given the increased frequency of cyberattacks. This is not a 'one size fits all' exercise though. Different organisations will need different measures in place to ensure that they are cyber secure. It is, therefore, important to get specialist legal advice from cyber experts when reviewing your cybersecurity practices. Your legal advisors can advise you on where the gaps are in your cybersecurity practices and what measures you should implement to bolster your cyber process and systems.

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