Press release

Date	1 October 2020
Contact	Andrea Moseley
	a.moseley@hlb.global
	+44 (0) 20 7881 1108
Pages	02

Remote working leads to increases in cyber attacks

LONDON – Global businesses have seen cyber-attacks rise as the world continues adjusting to remote working practices brought on by COVID-19, with 65% of organisations noting they have either been breached or exposed to an attack. That's one of the key findings from HLB's Cybersecurity Report which launched today.

From mobile security threats to unauthorised access to files, recent cyber-attacks shed light on an increasing problem. Cyber-attacks not only disable programs and steal data, but they can also include reputational damage, financial losses, and disruptions to business operations. While 65% of our respondents noted their organisation had been targeted, a worrying figure of 35% responded that they had not noticed a difference, potentially raising the question of had a potential breach been missed?

Commenting on the findings, Abu Bakkar, HLB's Chief Innovation Officer, says: *"COVID-19 has demonstrated how important technology is for business leaders, but the pandemic has truly highlighted the critical role cybersecurity plays. CEOs must work closely with their CTOs and IT consultants and recognise the investment needed in this area and build it into your business strategy. Without cybersecurity at the heart of your organisation, can you truly deliver for your customers?"*

Cyber attacks on the rise in 2020

Our experts overwhelming opinion is that phishing attacks are increasing, and highlight that social engineering is also rising. The impact of social isolation is also playing a key role in the rise in cyber-attacks as remote workers do not have their colleagues to double check any potential queries.

Challenges to making home offices secure

At the start of the pandemic, CTOs and IT management scrambled to get remote workforces running, facing vulnerabilities across several areas such as securing personal devices to giving access to virtual private networks (VPNs). These vulnerabilities allowed for cyber-attacks and data breaches to take place, leading to 88% of respondents noting that their companies changed their cybersecurity strategies and protocols.

Strengthening cyber-risk management strategy

When asked about the level of security across the three tenets of information security, one in five respondents doesn't believe their online systems are secure. HLB's Global Advisory Leader, Jim Bourke points out much of this is due to "*the fact that our workers*

are still working remotely and touching confidential data, so there continues to be exposure. From a cybersecurity month perspective, it's worth noting that the question about data confidentiality should have been answered with 100% secure. We have rules and regulations, like GDPR, so we should be secure. However, the rapid shift to remote working and with such a large portion of the workforce still working from home, many organisations have just not been able to fully comply in the short space of time." To manage cyber-risk, it's necessary to adapt the three tenets of information security of **data availability, data confidentiality** and **data integrity** to remote working environments.

Lessons learned from lockdown

When the pandemic hit, business leaders' priority was business continuity. However, the cyber-risk management lessons learned continue to build on the common themes of agility and resilience. The lessons business leaders should be aware of are:

- Improve cybersecurity training and support
- Don't wait to prepare IT infrastructure and cybersecurity protocols
- Think long-term relief not short-term solutions
- Regularly assess cloud computing threats and vulnerabilities
- Addressing cyber risk is an organisation-wide exercise.

ENDS

About our research

Between August and September 2020, we surveyed 76 IT professionals about their perceptions on information security and data protection in today's complex digital environment. Responses were collected via an online survey.

For further information on HLB's Cybersecurity Report, interview enquiries and high-resolution images, please contact Andrea Moseley, Marketing & PR Manager.

About HLB

HLB International is a global network of independent advisory and accounting firms. Formed in 1969, we service clients through our member firms in 158 countries, with 30,000 partners and staff in 795 offices worldwide.

Learn more about us and tell us what matters to you by visiting www.hlb.global