Press release

Date	11/10/2022
Contact	Rita Carolan
	r.carolan@hlb.global
	+44 (0) 20 7881 1100
Pages	02

78% of senior IT professionals believe their organisations are not prepared for cyberattacks

LONDON – Human behaviour is the greatest barrier to cybersecurity with most data breaches being linked to human error according to *HLB's Cybersecurity Report 2022,* published today. Whilst only 7% of respondents surveyed as part of this research believe there has been a decline in cyberattacks over the past 12 months, 78% expressed concern that their organisation is not fully prepared for an attack.

In September 2022, HLB surveyed 753 senior IT professionals via an online questionnaire about the challenges they face in today's cyber-risk landscape. The feedback shows that there are still considerable knowledge and competency gaps when it comes to cybersecurity. To help, this report also provides a framework to further develop cybersecurity practices to better prepare business in the event of an attack.

Commenting on the report, Abu Bakkar, HLB's Chief Innovation Officer said,

"Our research has shown that digital transformation has changed the way we work. In many cases this has opened us to a greater risk of cyberattacks due to the pace of technology adoption, resulting in a lag in training, awareness and contingency planning. Businesses, now more than ever, need to invest in more robust frameworks and training programs to protect their employees and the longevity of their business from the negative impacts presented by the ever-evolving cyber-environment"

Main findings include:

Skills Shortage

Employers are struggling with a labour market where access to talent has become challenging. When it comes to talent with strong cybersecurity skills this is no different. 85% of respondents see these skills shortages as a risk to cybersecurity. Similarly, 70% of respondents are also concerned about the lack of training on the subject. The combination of the rapid speed of technological advances, as well as the demand for people with technical data security backgrounds, has created a shortage of such skills. Continued learning is a must. There needs to be agreement from leadership that developing strong cybersecurity defence capabilities is an essential part of the business and needs investment. Organisations also need to look at more holistic approaches to employee retention which will help to keep cyber-talent in-house.

Cloud vulnerabilities and advance technology

Hybrid working, enabled by cloud capabilities and the ever-evolving flow of advanced technology, all makes for a cyber-environment that is difficult to control. Although 81% expressed concern over cloud vulnerabilities, it is here to stay. Migrating technology to the cloud is something HLB does for clients and provides awareness training and best practice implementation along the way. For a business to survive today, it is imperative to invest in cybersecurity and ensure there is a continuity plan in place for the likelihood of a future attack.

Human behaviour

The report found that 77% of respondents felt there was a lack of cybersecurity awareness from their staff. Whilst human behaviour takes time to change this is not the case for cyberattacks which keep evolving at a fast pace to become more sophisticated. Hybrid and remote working have made employees easier targets. To change the human psyche, there needs to be an emphasis on constant training and internal awareness about the cost of vulnerability, demonstrating the negative impact of the data breaches and business disruption caused by cyberattacks.

Jim Bourke, HLB Global Advisory Leader said,

"Cybersecurity is one of the biggest threats to our society today and it is worrying that so many respondents are not prepared for a cyberattack. You cannot wait for an attack to then prepare for the next one. Businesses need to be meeting with cyber professionals to figure out how to exercise best practice to ward off an attack. Plans are only part of the preparation, human implementation is crucial, you must continually test existing cybersecurity procedures, running penetration tests and drills. Only through doing all this, can your business continue to thrive for the long-term."

Read the full report **here**.

END

About HLB

HLB International is a global network of independent professional accounting firms and business advisers. Formed in 1969, we service clients through our member firms in 157 countries, with 38,732 partners and staff in 1,030 offices worldwide.

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