Cyber attacks are on the rise as security risks inherent in working from home are being exploited

Published 4 August 2020

A recent report released by insurance company, Hiscox, outlined that 41% of Irish businesses experienced at least one cyber attack in the six month period from September 2019 to February 2020. The report was conducted in respect of over 5,500 companies across eight countries, including France, Germany, the UK and Ireland. The report found that the sectors most affected by cyber attacks are the energy, manufacturing, financial services, telecoms and pharmaceuticals industries. It reported that 6.5% of Irish companies surveyed had paid a ransom following a ransomware attack. However, it wasn't all bad news, as the report indicated that Ireland topped the "readiness" table with 89% of companies surveyed having either a dedicated head of cyber security or a dedicated team to deal with cyber incidents.

Elsewhere, it was reported by the Law Society that the Solicitors Regulation Authority ("SRA") in the UK warned that cyber hackers were specifically targeting solicitors who were working from home and handing sensitive client information or large sums of money. The SRA reported that in one incident, a cyber criminal had attempted to set up a monthly Stg£4,000 standing order from a firm's client account. It is clear that hackers have identified the security risks inherent in home working and are attempting to exploit these weaknesses. The Law Society advised that at a minimum, work laptops and devices should be encrypted and systems should be installed to track and delete data if devices are lost or stolen.

These reports demonstrate the increasing risk of cyber attacks for Irish and international companies alike, with fraudsters becoming more sophisticated and prolific than ever before. Conversely, however, it is clear from the Hiscox report that there is a growing awareness amongst businesses of the importance of cyber security expertise and having a cyber security policy in place to deal with cyber incidents and attacks. In addition, the Data Protection Commission's annual report for 2019 demonstrates an increasing awareness amongst data controllers, processers and data subjects of their rights and obligations under the GDPR.

It is imperative that all companies have comprehensive cyber security and data protection policies in place together with a clear understanding of their rights and obligations under data protection legislation. Undoubtedly, the recent news stories will have come as a salutary reminder to all businesses in this regard.

A copy of Hiscox's report is available here.

If you have any questions in relation to this update, or would be interested in attending a webinar covering this topic in greater detail, please contact us and we would be delighted to assist.

Authors

Lisa Broderick
Dublin
+353 (0) 1 231 9683
lbroderick@dacbeachcroft.com

Rowena McCormack
Dublin
+353 (0)1 231 9628
rmccormack@dacbeachcroft.com

Julie-Anne Binchy
Dublin
+353 (0) 123 19636
jabinchy@dacbeachcroft.com

Charlotte Burke
Dublin
+353 (0)1 2319679
cburke@dacbeachcroft.com

Simon Halpin
Dublin
+353 (0) 123 19639
shalpin@dacbeachcroft.com

David Freeman
Dublin
+353 1588 2558
dfreeman@dacbeachcroft.com

DAC BEACHCROFT