EINPRESSWIRE

NEW RESEARCH: 3 in 5 organisations did not do enough to stay cyber secure during lockdown

51% of organisations admitted they did not have a remote working policy in place

ELY, UNITED KINGDOM, August 4, 2020 /EINPresswire.com/ -- A survey conducted by IT Governance Ltd and DQM GRC has found that 1 in 4 organisations did not provide any staff training on cyber risks or privacy threats related to remote working and COVID-19 before or during lockdown.

The research, which surveyed respondents from more than 200 organisations, also discovered that:
•30% of respondents do not feel confident they would always recognise a cyber incident. This is particularly concerning given that there has been a surge in cyber crime, such as phishing attacks, as criminals are taking advantage of the new vulnerabilities widespread home working presents.
•60% of respondents did not conduct a risk assessment on personal devices used for remote working before going into lockdown.
•18% did not have any training, policies or processes for remote working security before lockdown.
•58% of those surveyed did not run staff training on how to implement information security at home.
•More than half (51%) did not have a remote working policy in place.

Organisations struggled to adapt quickly

When asked about their experiences of adapting to the pandemic:

- 39% said they had difficulties adapting, with 4% confessing they have not coped very well at all.

- More than a third (36%) of respondents think that they will never go back to the way things were before lockdown, and nearly half (49%) believe they will go through several cycles of lockdown and eased restrictions.
- More than three quarters (77%) admitted that their organisation did not have a bring your own device (BYOD) policy that covered domestic equipment in a remote working environment, such as network routers, before lockdown.
- When asked if their organisation had adapted its policies and procedures to home working, 50% responded that it had or that it was not necessary, 38% said this was in progress, and 10% said it had not adapted them.

More to do on privacy by design

When asked whether privacy by design was important when buying and deploying new technology (such as video conferencing software) during lockdown, a third (33%) said that they were either more focused on getting operations set up quickly than considering the privacy implications of the new technology, or had not considered it at all.

Geraint Williams, Group CISO of GRC International Group, commented: “The lack of staff training around the cyber risks COVID-19 has presented for remote working is worrying, and we’ll have to wait and see what this results in for organisations further down the line when the potential cyber incidents that occurred during lockdown are discovered.

“There are huge consequences for not training staff on how to implement information security at home, and this should have been a priority for all organisations when a mass move to home working became evident. Click rates for phishing attacks sit at roughly 3%, and even the most digitally adept employees can fall prey to emails impersonating clients, suppliers or industry subscription services. If your staff are working remotely, outside of your organisation’s usual security perimeter, these incidents are even harder to detect – especially if they go unreported.

“When not implemented properly, remote working can also expose organisations to the insecurities of home networks and the potentially unsecure devices used by other household members, which employees may not recognise as hazardous. This means there is a huge increase in the risk of data breaches and cyber security issues, and this new reality makes security awareness and training even more important where working from home is concerned.”

Camilla Winlo, Director of Consultancy at DQM GRC, added: “The ICO [Information Commissioner’s Office] told organisations clearly that they have a responsibility to maintain data protection standards regardless of where individuals are working. The whole point of lockdown was to keep people safe, so it's disappointing to see that, in many cases, keeping people safe from coronavirus meant increasing their risk of a computer virus. We can't have a situation where people are put at risk of serious consequences like fraud and identity theft when they are already worried about their health and their jobs.

"We have seen Zoombombing incidents ranging from the funny to the frightening, and the NHSX track and trace app fail to get off the ground on schedule – all because of poor privacy by design practices on the part of the developers and equally poor procurement practices on the part of those who buy them. Privacy is not a 'nice to have' – it's a fundamental human right, and poor privacy practices are usually a good sign that corners are cut in other important areas, too.

"With home working now looking like a permanent and widespread feature of corporate life, it's essential that organisations act now to get up to speed – before it's too late."

IT Governance, the leading provider of cyber security and data privacy risk management solutions, has produced a suite of products and services in response to the data privacy and security risks presented by the COVID-19 lockdown and post-lockdown era.
The COVID-19 product suite contains a range of solutions, including remote working policies, remote compromise penetration testing, security staff awareness training for remote teams, business continuity support and a COVID-19 consultancy support service that delivers data privacy, cyber security and legal expertise in one contract.

To find out more about IT Governance's solutions can help your organisation visit the website here.

- ENDS -

Survey breakdown

DQM GRC and IT Governance surveyed 205 organisations based in the UK.

IT Governance Ltd and DQM GRC are GRC International Group companies

About IT Governance
IT Governance is a leading global provider of cyber risk and privacy management solutions, with a special focus on cyber resilience, data protection, the Payment Card Industry Data Security Standard (PCI DSS), ISO 27001 and cyber security.
IT Governance is committed to helping businesses protect themselves and their customers from the perpetually evolving range of cyber threats. Its deep industry expertise and pragmatic approach help clients improve their defences and make key strategic decisions that benefit the entire organisation.
IT Governance's Protect - Comply - Thrive approach is aimed at helping organisations achieve

resilience in the face of constant change.

About DQM GRC
DQM GRC’s award-winning range of services and solutions enables organisations of any size and across every industry to have confidence in their data.
Formed in 1996, DQM GRC was one of the first specialist consultancies dedicated to advancing all organisations’ data protection and governance capabilities.
Acquired by GRC International Group plc in March 2019, it is now part of a leading global supplier that boasts of an extensive one-stop shop for governance, risk and compliance products and services.

Cameron Toarke
GRC International Group
+44 7983 623 150
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/523140141