How lockdown has put cyber security awareness under the spotlight

The Department for Digital, Culture, Media and Sport (DCMS) has recently published its sixth annual report following a survey examining the threat of cyber security breaches in businesses, charities and educational institutions (DCMS Report).

The survey which was conducted during 12 October 2020 to 22 January 2021, recognised the impact the coronavirus pandemic (COVID-19) has had on cyber security risk for businesses in the United Kingdom (UK) with the transition from physical to remote working potentially expediting planned cyber security investment. This article will summarise the key findings and messages identified in the DCMS Report.

**Awareness and attitudes and the impact of COVID-19**

Understandably the impact of the pandemic was a big factor in the survey results. The DCMS Report indicated that many organisations adopted new security solutions through the pandemic, including cloud security and multi-factor authentication and VPN connections to access files. It is unclear how much of the shift arose directly from the pandemic itself. It is likely that some of the investment would have been planned as part of more a cultural shift to more flexible working and was accelerated as a response to the pandemic.

Overwhelmingly, 84% of businesses maintained that the pandemic had not changed their cyber security risk priorities. Where businesses did indicate a change in priorities, 14% placed cyber risk as a higher priority and 2% as a lower priority. Overall businesses suffered an increase in the number of cyber-attacks, especially phishing attacks.

Returning to the businesses that had not changed their prioritisation as a result of the pandemic, many felt that their cyber security risks were sufficiently managed with a number citing a well-established agile working culture. Some businesses interviewed stressed the survival of the business was their main priority during the early stages of the pandemic and/or that they simply did not have the time to review their cyber security measures during this time.

**Specific challenges**

The DCMS Report identified some challenges relating to the cyber security during the pandemic which included:

- Remote working resulting in a greater reliance on staff to correctly follow procedures and remain vigilant
- Increased costs of licences of remote user monitoring software were too high for some businesses to install
- Dealing with hardware and software changes and upgrades was more difficult, particularly for larger organisations
- Supplying IT equipment to staff and upgrading systems
- Stretched resources leading to conflicting priorities between IT service continuity, maintenance work, and cyber security management
- Reduction in personnel due to the lockdown restrictions made it harder to conduct cyber security awareness training

---

Senior management awareness
The DCMS Report confirmed that 77% of the businesses surveyed stated that senior management recognised cyber security as a high priority risk. It was also commented that cyber security was being discussed more in boardrooms than when the survey was first conducted suggesting an increase in cyber security awareness. This continues to be a year on year trend which is reassuring.

The findings also show that senior management/board members of businesses were receiving regular updates on the state of their cyber security and actions taken, either monthly (15%), quarterly (18%) or annually (14%) or when a breach occurs (4%) which suggests the message about the importance of identifying monitoring and managing cyber security risks and the awareness is having an impact.

Sector differences
The following business sectors attached a higher priority to cyber security:

- Finance and insurance: 72%
- Information and communications: 62%
- Health, social work and social care: 56%

This view is consistent with previous reporting periods.

Training and broader cyber awareness
14% of businesses ensured that staff received training within the last 12 months about the threats and vulnerabilities of cyber security, the majority of these businesses were medium to large size organisations (38% and 47% respectively). The sectors most likely to offer training were the finance and insurance sector and information and communications. Conversely entertainment, service and membership organisations, construction, utilities and production, and the retail and wholesale sectors were less likely to offer training.

In addition to the above, awareness of the Government’s initiatives has also gradually increased year on year. These include:

- 14% Cyber essentials
- 34% Cyber aware
- 18% NCSC 10 steps guidance
- 14% NCSC guidance for moving business online
- 21% Home working and video conferencing guidance

There was a greater awareness of these initiatives in the medium to larger sized businesses.

These initiatives act as a helpful reminder to assist organisations check what actions they have taken, especially around backups, user access and patch management as well as offering guidance to employees, and can assist with managing risk and compliance.
The NCSC guidance is that system and email passwords should be changed regularly and should be strong, consisting of three random words mixed with special characters and numbers. It is appreciated that doing so may make it more difficult to remember passwords but with 27% of UK citizens adding more than four new password-protected accounts to their systems over the last 12 months, and even more alarming is that 6% of the people in the UK are still using “password” as their password, it is vital that passwords are set so that they are difficult to hack.

Cyber security attacks and breaches
39% of businesses reported experiencing a cyber security breach or attack in the last 12 months. The higher percentage of those occurring in medium to larger size organisations. Of those organisations the following types of breaches/attacks were identified:

- 83% Phishing attacks (91% consists of larger firms)
- 27% Others impersonating organisation in emails or online
- 9% Viruses, spyware or malware (excluding ransomware)
- 8% Denial of service attacks
- 8% Hacking or attempted hacking
- 7% Takeovers of organisation’s or users’ accounts
- 7% Ransomware
- 2% Unauthorised accessing of files or networks by outsiders
- 2% Unauthorised accessing of files or networks by staff
- 1% Unauthorised listening into video conferences or instant messages
- 5% Any other breaches or attacks

The top three causes have remained consistent since the question was first asked back in 2017. Phishing attacks are still considered to be the most disruptive type of attack facing businesses. 51% of businesses reported that they were experiencing breaches or attacks at least once a month if not more often.

On a positive note the findings suggested that businesses were becoming more resilient to cyber security breaches, with 71% of businesses stating that it took them no time at all to recover from an incident. The average cost to businesses of all breaches or attacks over the last 12 months is now £2,670 (average staff time cost is £740) which is an increase on previous years, emphasising the financial damage a cyber security breach or attack can have on a business. 62% of businesses will take positive action following a cyber security incident which includes a combination of new technical controls and further training or communications to employees.

**Cyber Insurance**

43% of businesses reported having some form of cyber insurance cover in place, an increase of 11% from last year, when this question was first asked. 37% of businesses reported that they had cyber security cover as part of a wider insurance policy and 6% of businesses confirmed that they held a specific cyber security insurance policy, this was more likely in medium and larger size businesses.

Insurance cover was more prevalent in the finance and insurance sector. 60% of these types of businesses had some form of coverage against cyber security breaches followed by information and communications (57%), health, social care and social work (53%) and professional, scientific and technical firms (53%). The reasons given for taking out some form of cyber insurance cover was because:

- the threat of significant cyber security breach could cause the business to cease trading
- there were insufficient monies to fund recovery
- the business did not have the specialist skills required to deal with incident response and potential reputational damage
- clients were increasingly requesting cover in contracts
- the comfort of fines being covered in the event of a personal data breach

In Summary

To summarise, this is the first Cyber Security Breaches Survey to be undertaken since the start of the pandemic. The Government imposed lockdown restrictions brought about many changes in working practices and environments and it is be helpful to see how businesses have responded to cyber security risks during Covid-19.

Overall, the findings are generally consistent with previous years, cyber security risk awareness remains steady but there has been an increase in awareness by senior management and board members. There has also been an increase in businesses taking out some form of cyber insurance cover, with the key factors behind this being the existential threat of a cyber security incident to the business organisations, and the costs of funding recovery, or having the requisite skills and expertise to deal with such incidents and to protect against reputational damage.

Whilst we can take comfort from the findings, as always there is room for improvement. The pandemic has highlighted the need to review existing measures and test their effectiveness to ensure that they are fit for purpose, especially as some businesses have had to prioritise between IT service continuity, maintenance and managing cyber security. Overall, the general consensus is that businesses recognise the need for increased cyber security risk awareness and want to make cyber security management an integral component of their business continuity and operational resilience planning.

For further information please contact:

Joanne Cracknell MSc LLB (Hons)
Associate Director, FINEX Global
+44 117 976 9376
+44 7584 683 012
Joanne.Cracknell@WillisTowersWatson.com

---

43% of businesses reported having some form of cyber insurance cover in place, an increase of 11% from last year, when this question was first asked.

62% of businesses will take positive action following a cyber security incident.
About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.