Press release: UK Boards of biggest firms must do more to be cyber aware

- Many FTSE 350 boards still don't understand the impact of a cyber attack on their business
- Incident plans are in place but are not tested thoroughly enough
- New measuring tool will help firms manage their cyber risk more effectively

Boards at some of the UK's biggest companies still don't fully understand the potential impact of a cyber attack according to a new report.

The Government's Cyber Governance Health Check looks at the approach the UK's FTSE 350 companies take for cyber security. The 2018 report published today shows that less than a fifth (16%) of boards have a comprehensive understanding of the impact of loss or disruption associated with cyber threats. That's despite almost all (96%) having a cyber security strategy in place.

Additionally, although the majority of businesses (95%) do have a cyber security incident response plan, only around half (57%) actually test them on a regular basis.

Digital Minister Margot James said:

> The UK is home to world leading businesses but the threat of cyber attacks is never far away. We know that companies are well aware of the risks, but more needs to be done by boards to make sure that they don't fall victim to a cyber attack.
>
> This report shows that we still have a long way to go but I am also encouraged to see that some improvements are being made. Cyber security should never be an add-on for businesses and I would urge all executives to work with the National Cyber Security Centre and take up the government's advice and training that's available.

Awareness of the threat of cyber attacks has increased. Almost three quarters (72%) of respondents acknowledge the risk of cyber threats is high, which is a big improvement of only just over half (54%) in 2017.

The implementation of the General Data Protection Regulations (GDPR) in 2018 has had a positive effect in increasing the attention that boards are giving cyber threats. Over three quarters (77%) of those responding to last years health check said that board discussion and management of cybersecurity had increased since GDPR. As a result over half of those businesses had also put in place increased security measures.

Ciaran Martin, CEO of the NCSC, said:

> Every company must fully grasp their own cyber risk – which is why we have developed the NCSC’s Board Toolkit to help them. This survey highlights some urgent issues companies will be able to address by putting our Toolkit’s advice into practice.

> Cyber security is a mainstream business risk, and board members need to understand it in the same way they understand financial or health and safety risks.

Meanwhile, more work is being done to improve the cyber resilience of business, and a new project has been announced that will help companies understand their level of resilience. The cyber resilience metrics will be based on a set of risk-based principles to allow firms to measure and benchmark the extent to which they are managing their cyber risk profile effectively.

Once developed these indicators will provide board members with information to understand where further action and investment is needed.

Government is recommending the Boards continue to make improvements to their cyber security. This includes using the guidance published by the National Cyber Security Centre (NCSC) to improve the management of risks.

Companies should also ensure that cyber risks are taken into account in their business strategy and appoint a Chief Information Security Officer (CISO) or other appropriately placed staff members who can clearly communicate information about cyber risks to the board.

Notes to editors:

1. Read the 2018 FTSE 350 Cyber Governance Health

2. DCMS’s Cyber Governance Health Check is part of the Government’s National Cyber Security Strategy: 2016-2021 to make the UK the safest place to live and do business online. It is backed by £1.9 billion investment over five years.

3. The 2018 FTSE 350 Cyber Governance Health Check was undertaken in partnership with Winning Moves and support from EY, KPMG, PwC and Deloitte who have worked with their FTSE 350 clients to participate in the survey.

Additional quotes

Richard Horne, cyber security partner at PwC said:

> Boards need to recognise that they have a responsibility to drive changes to business and IT operating models to enable their organisations to be securable. Managing cyber risk is about far more than just building security controls, and requires board-driven business change.

> At PwC, we work with a variety of organisations and there’s always a noticeable difference in those who have a strong understanding of cyber risk at board level.

Gavin Cartwright, Associate Partner, Cyber security at EY said:

> With only 1 in 5 FTSE 350 companies undergoing a cyber simulation last year, the report highlights that cyber security is still not fully embedded in the culture of many of these companies. In addition to having cyber security strategies in place, organisations and their boards need to continually build and invest in their in-house capabilities, practice responses and train and evaluate cyber-first responders across their business and supply chain.

Kevin Williams of the KPMG UK cyber security practice said:

> Cyber security is a business issue, not an IT issue. Some of the more successful companies ensure regular reporting on cyber risks directly to the board, creating clear line of sight between the business and the risk. They also ensure regular testing of their capabilities to respond to information security incidents.

> The 2018 survey shows that we are moving in a positive direction, but there continues to be a need for a more comprehensive understanding of the impact of loss or disruption associated with cyber threats to an organisation. The investment needs to be not only financial but in education for all and ensuring the right resources are in place to innovate, take advantage of new technological advances, whilst assessing the risks and responding accordingly.