Press release: Two in three bosses at Britain's biggest businesses not trained to deal with a cyber attack

- New reports highlight scale of the cyber security and data protection challenge
- One in ten FTSE 350 companies operate without a response plan for a cyber incident
- Only six per cent of businesses completely prepared for new data protection rules
- Separate new research finds charities are as susceptible to attacks as businesses Undertaken in the wake of recent high profile cyber attacks, the survey of the UK's biggest 350 companies found more than two thirds of boards had not received training to deal with a cyber incident (68 per cent) despite more than half saying cyber threats were a top risk to their business (54 per cent).

One in ten FTSE 350 companies said they operate without a response plan for a cyber incident (ten per cent) and less than a third of boards receive comprehensive cyber risk information (31 per cent).

Minister for Digital Matt Hancock said:

> We have world leading businesses and a thriving charity sector but recent cyber attacks have shown the devastating effects of not getting our approach to cyber security right.
>
> These new reports show we have a long way to go until all our organisations are adopting best practice and I urge all senior executives to work with the National Cyber Security Centre and take up the Government's advice and training.
>
> Charities must do better to protect the sensitive data they hold and I encourage them to access a tailored programme of support we are developing alongside the Charity Commission and the National Cyber Security Centre.

There has been progress in some areas when compared with last year's health check, with more than half of company boards now setting out their approach to cyber risks (53 per cent up from 33 per cent) and more than half of businesses having a clear understanding of the impact of a cyber attack (57 per cent up from 49 per cent).

The Government is fully committed to defending against cyber threats and a five-year National Cyber Security Strategy (NCSS) was announced in November 2016, supported by £1.9 billion of transformational investment. This includes opening the National Cyber Security Centre and offering free online advice as

well as training schemes to help businesses protect themselves.

The 10 Steps to Cyber Security guide sets out a comprehensive framework to help company boards manage cyber risks, from getting the basics right through to protecting their most critical assets, and the Cyber Essentials scheme sets out the technical basics all companies should have in place.

Earlier this week, Government also announced proposals on how to help the nation's essential industries be more resilient to cyber threats through the NIS Directive.

Alex Dewdney, NCSC Director for Engagement, said:

> The NCSC is committed to making the UK the safest place in the world to live and do business online.
>
> We know that we can't do this alone – everyone has a part to play. That's why we're committed to providing organisations with expert advice through our website and direct engagement.
>
> We also urge organisations to follow the guidance in the Government's Cyber Essentials Scheme.

Separate new research looking at the cyber security of charities has also been published today.

It found charities are just as susceptible to cyber attacks as businesses, with many staff not well informed about the topic and awareness and knowledge varying considerably across different charities. Other findings show those in charge of cyber security, especially in smaller charities, are often not proactively seeking information and relying on outsourced IT providers to deal with threats.

Where charities recognised the importance of cyber security, this was often due to holding personal data on donors or service users, or having trustees and staff with private sector experience of the issue. Charities also recognised those responsible for cyber security need new skills and general awareness among staff needs to raise.

Helen Stephenson CBE, Chief Executive at the Charity Commission for England and Wales, said:

> Charities have lots of competing priorities but the potential damage of a cyber-attack is too serious to ignore. It can result in the loss of funds or sensitive data, affect a charity's ability to help those in need, and damage its precious reputation. Charities need to do more to educate their staff about this threat and ensure they dedicate enough time and resources to improving cyber security.

> We want to make sure charities are equipped to do this, and we encourage them to use the advice on our Charities Against Fraud website. We also continue to work closely with the Department for Digital, Culture, Media and Sport to help charities protect themselves online.

The FTSE 350 Cyber Governance Health Check is the Government's annual report providing insight into how the UK's biggest 350 companies deal with cyber security.

The Government will soon be introducing its new Data Protection Bill to Parliament. With this coming into effect next May, implementing the General Data Protection Regulation (GDPR), the report for the first time included questions about data protection.

The new data protection law will strengthen the rights of individuals and provide them with more control over how their personal data is being used.

The report found:

- Awareness of GDPR was good, with almost all firms (97 per cent) aware of the new regulation
- Almost three quarters (71 per cent) of firms said they were somewhat prepared to meet the GDPR requirements, with only 6 per cent being fully prepared
- Just 13 per cent said GDPR was regularly considered by their board
- 45 per cent of Boards say they are most concerned with meeting GDPR requirements relating to an individual's right to personal data deletion

The Information Commissioner's Office has produced guidance for organisations on implementing the regulation, including a checklist for businesses on the actions they need to take; and a series of interactive workshops and webinars.

The ICO will also produce guidance for organisations about the responsibilities under the GDPR and individuals on their rights under the GDPR. The Department for Digital, Culture, Media and Sport will continue to work closely with the Information Commissioner's Office (ICO) during this transitional period.

Note to editors:

Media enquiries – please contact the DCMS News and Communications team on 020 7211 2210 or out of hours on 07699 751153.

The FTSE 350 Cyber Governance Health Check is carried out in collaboration with the audit community, including Deloitte, EY, KPMG and PWC: https://www.gov.uk/government/publications/cyber-governance-health-check-2017

The Cyber Security Among Charities report covers the findings from qualitative research undertaken with UK registered charities: https://www.gov.uk/government/publications/cyber-security-in-charities

The Department for Digital, Culture, Media & Sport (DCMS) has commissioned the UK Cyber Security Sectoral Analysis Survey to provide statistics about the size, scale and future opportunities for the UK's Cyber Security industry.

The reports are part of the Government's £1.9 billion investment to significantly transform the UK's cyber security. The National Cyber Security Strategy sets out how the UK Government will deliver a UK that is secure and resilient to cyber threats; prosperous and confident in the digital world. The National Cyber Security Programme managed by the Cabinet Office coordinates the work undertaken to implement the UK's National Cyber Security Strategy. Further information is available at www.gov.uk/cybersecurity

Annex

Paul Taylor, UK head of Cyber Security at KPMG, said:

"Cyber-attacks continue to pose a growing threat to business. While cyber security has cemented itself onto the board's agenda, they often lack the training to deal with incidents. This is hugely important as knowing how to deal confidently with an incident in the heat of the moment can save time and money. The aftermath of a cyber-attack, without the appropriate training in managing the issue, can result in reputational damage, litigation and blunt competitive edge."

Zubin Randeria, cyber security leader at PwC, said:

"The report's findings echo those of the PwC CEO Survey, which found that three-quarters of UK CEOs consider cyber risks to be a significant threat to their business and 97% are addressing cyber incidents. It's positive that cyber security is now front of mind for boards and business leaders, but concerning that many still are not equipping themselves with the right knowledge to respond when the worst does happen. Cyber security attacks are now an everyday reality and it's the responsibility of business leaders to make sure they're prepared.

"The most successful leaders will be those who take an active involvement in cyber security governance and set the tone from the top – this is not an issue just to delegate to more technical teams. Investors, customers, the media and the general public all routinely scrutinise companies' responses to cyber security incidents, as we've seen from the recent ransomware attacks. Companies that fail to prepare to respond to a breach also leave themselves exposed to a damaging commercial and reputational backlash."

Phill Everson, head of cyber risk services at Deloitte, said:

"This year's report marks a clear improvement in board level awareness of cyber risks and their impacts, driven in large part by high profile, cross-sector incidents. There is still some way to go, though, as the findings show that many boards still do not have a defined role to lead a company-wide response. This corroborates with recent Deloitte analysis of FTSE 100 annual reports, which found that just 5% disclose having a board member with

specialist technology or cyber experience.

“As well as greater awareness of the financial and reputational impact of a cyber breach, preparedness is also key to a successful response. From May next year, cyber breaches will have to be reported within 72 hours under General Data Protection Regulation (GDPR). This is significantly sooner than the period that many companies have historically alerted customers, which often runs into many months. As hackers become increasingly more sophisticated, companies will have to ensure that staff training and technology stays ahead of the evolving cyber threat to respond in a timely and effective manner.”

Stuart Whitehead, UKI Head of Cybersecurity, Privacy & Resilience at EY said:

“Cyber is an ever increasing threat to the UK economy and although we are glad to see that this latest survey of the UK’s largest organisations illustrates that cyber is increasingly a board level priority, there is still some way to go to best prepare organisations for a potential breach. With the current backdrop, the cyber agenda is evolving into a conversation about organisations’ resilience to cyber-attacks. This is not only how organisations protect themselves but how they respond to an incident, recover business processes and limit the impacts to revenue and reputation. The increase in Board level attention is encouraging, but greater emphasis will be required over the coming years to truly improve the security posture of organisations across the UK.”