FTSE 350 CYBER SECURITY

In an increasingly digital world, global business is under growing pressure to improve its information security and cyber-governance. As the UK government's recent £1.9 million investment in the issue accentuates.

WHAT'S THE RISK?

The security of, or potential damage to, systems, networks & data in cyber-space, as well as the hardware that they are stored upon. This can have significant impact on information security, economic factors, as well as reputational concerns.

Sector Trends

100% Twice as many sectors now recognise cyber- security risk in their assessments

Now including Forestry & Paper (2015: 0%), and Software & Computer Services (2015: 67%)

0% Industrial Metals & Mining still score 0%

Technology, Hardware & Equipment, and Tobacco now score 0% too (2015: 67% and 50% respectively)

Responsibility

38% of companies who recognise cyber-security as a key risk have a dedicated Board Risk Committee (2015: 33%)

55% of companies with a risk committee combine this responsibility with those of another, typically audit-dedicated

3 companies have a combined sustainability & risk committee

easyJet plc Has a dedicated IT Governance & Oversight Committee for cyber-security

Recognition

Cyber security remains a high priority ESG risk, still 2nd only to regulatory compliance (79% v. 84% overall recognition)

This is as much as market recognition of health & safety, & poor ethics impact as risks, combined (45%, 33% respectively)

19% of FTSE 350 companies DO NOT recognise cyber- security amongst their key risks

EU GDPR Regulation 2016/679

EU strengthens existing cybersecurity regulations: regulation enters into application 25 May 2018

Adopted by the European Parliament April 2016, the General Data Protection Regulation (GDPR) is intended to strengthen & unify existing strategies within the EU & extends the law's scope to all foreign companies processing data of EU residents.

PAYPAL - TWITTER - SPOTIFY

October 2016 saw these big-name services frozen by a significant DDoS hack in USA

Use of internet-connected devices to hack the 'internet switchboard' company, Dyn Inc, this denial-of-service attack prevented service access from a number of big-name US companies.

PayPal apologized for the inconvenience and declared that networks had not been hacked. ?

NEW (YORK) REGULATIONS

New York first in US to propose cyber security regulation: due 01 January 2017

Covering banks, insurance companies, and other financial service providers, this New York Dept. of Financial Services (NYDFS) regulation requires the recognition of, & internal reporting on, cyber-security risks & management strategies.

References

NY DFS (2016) 'Cybersecurity Requirements for Financial Services Companies' (http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf) New York: State Department of Financial Services <04 Nov 2016>

EU Commission (2016) EU Commission: Reform of EU data protection rules [online] (http://ec.europa.eu/justice/data-protection/reform/index_en.htm) <04 Nov 2016>

Menn, J., Finkle, J. & Volz, D. (2016) 'Cyber attacks disrupt PayPal, Twitter, other sites' Reuters [online] (http://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME) <04 Nov 2016>

Email: Info@manifest.info | Tel : + 44 (0)1376 503500