Cybersecurity is the defining business challenge of the 21st century

blogs.lse.ac.uk/businessreview/2017/03/28/cybersecurity-is-the-defining-business-challenge-of-the-21st-century/

3/28/2017

Speaking in 1941, a renowned businessman said “I believe that every right implies a responsibility; every opportunity, an obligation; every possession, a duty.” While **John D Rockefeller** was speaking at a time when the likes of drones, driverless cars and virtual reality were distant dreams and works of fiction – the central tenet of the quote is firmly applicable to the dilemma businesses face today when engaging in the “digital revolution”.

For every opportunity that the digital world presents to business, there must also be recognition of the obligation to protect their organisation and customers from the pitfalls of such an interconnected world. The rewards presented by the digital revolution are clear: more than 12 per cent of GDP now comes from the digital economy. From creating whole new industries to making existing ones more efficient, it is difficult to imagine a business operating today without some sort of digital footprint. It is right that businesses should be embracing this new world, but they must do so responsibly.

As the IoD’s new report on Cyber Security argues, such is the scale of the cybercrime challenge that the defining business challenge of the 21st century will be to ensure that data, bank accounts and intellectual property remain secure. According to ONS figures, there were 5.6 million fraud and computer misuse crimes in the first half of last year. For an individual business, the financial and PR implications of an attack can be devastating.

The likes of Sony or Talk Talk (two of the more notable public attacks of late) can of course weather such a breach, given their size. It is difficult to imagine an SME recovering in the same way. Nor should smaller companies think that their relative anonymity in comparison to a FTSE company or large state institution protects them from nefarious web users. Hackers do not discriminate, attacks can take place everywhere from multinational companies to local councils. When individuals’ personal information is at stake, this is an issue for everyone and every organisation

The opportunities and the risks are apparent. The tension lies in where the responsibility sits. As a recent study by a

FTSE 100 company shows, whilst boards believe responsibility falls to the IT team, IT teams themselves believe the opposite. Cyber security is of such critical importance that it has to be viewed as a principal business risk. The responsibility to set strategy, plan the response and ensure compliance with regulation *has* to sit with the board, as it does with other profit or loss decision-making.

The impact of an attack is no longer confined to just the fallout of the crime. From April 2017 all organisations will be obliged to report a data breach to the relevant authority or face fines up to €10 million or 2 per cent of global turnover. This is just one aspect of the regulations being brought in through the General Data Protection Regulation (GDPR). Company directors need to get up to scratch with this regulation and routinely assess the threats they face.

Government statistics from 2015 show that whilst 49 per cent of businesses in FTSE 350 place cyber as a top risk, only 16 per cent of boards have a clear understanding of where and how the company's key information is shared with third parties. The IoD's report shows that of the business leaders surveyed, 94 per cent saw cyber security as important, but only 56 per cent had any formal strategy for cyber security in place; a worrying mismatch.

The importance of technical expertise, or, at a minimum, understanding, at the board level cannot be understated. Risk in business is as old as business itself and the digital revolution is merely another development for companies to contend with and try to capitalise on.

Anyone with a stake in a business should be interested in their cyber security arrangements. For listed companies, this means that shareholders will increasingly interrogate boards on the issue as they would on financial results or remuneration. For companies of all sizes, it means that suppliers and customers will demand more transparency on how firms are protecting their systems and data. Ultimately, the advantages of digital technology heavily outweigh the risks, but we must go forward with our eyes open, prepared for the challenge.

♣♣♣

Notes:

- *This blog post is based on Cyber security: Ensuring business is ready for the 21st century, by Richard Benham, IoD Report, March 2017*
- *The post gives the views of its author, not the position of LSE Business Review or the London School of Economics and Political Science.*
- *Featured image credit: Password security, by carlosalbertoteixeira, under a CC0 licence*
- *Before commenting, please read our Comment Policy.*

James Jarvis is Corporate Governance Analyst at the Institute of Directors. Prior to this role he worked as Special Adviser to the IoD Chairman, Lady Barbara Judge CBE, and before this worked within the IoD Institute Secretaries Office. James is a Politics graduate from Manchester Metropolitan University.