A new cyber frontier

November 2016

Earlier this month Philip Hammond launched the UK's new cyber strategy which aims to make the UK 'one of the safest places to do business in the world'. The strategy is built on three core pillars: defend, deter and develop; and is underpinned by a £1.9 billion investment.

High profile breaches such as Yahoo and Tesco Bank regularly remind organisations that cyber security is one of the top threats facing businesses today. Recent estimates put the global cost of cyber-crime at $445 billion (World Economic Forum's 2016 Global Risks Report), and the threat (and cost) is only set to increase as more infrastructure, services and devices become 'connected' and therefore vulnerable to attack.

The UK's new cyber strategy, launched on 1st November, sets out how the Government intends to protect its citizens and the economy in the face of this increasing threat. It also provides an updated assessment of the current threat landscape (providing short case studies on recent cyber breaches such as TalkTalk) and the vulnerabilities faced by the UK (including in relation to unpatched legacy systems and the Internet of Things).

The strategy builds on the initiatives, institutions, funding and funding promises (George Osborne had announced the £1.9 billion investment last November) established under the Government's previous cyber strategy, launched in 2011. It centres around three pillars (see box *The strategy's three core objectives*), and is supported by the UK's new National Cyber Security Centre (NCSC). The NCSC, which opened this October, is the Government's central national body for cyber security. As well as managing major incidents, it aims to make it simpler for businesses to get advice on cyber security (for example, it will produce guidance) and to interact with Government on cyber security issues.

The strategy's three core objectives:

1. **Defend:** strengthen the defences of Government, critical national infrastructure sectors (like energy and transport) and our wider economy. "In practice this means Government taking a more active cyber defence approach."

2. **Deter:** deter cyber actors by strengthening law enforcement capabilities to raise the cost and reduce the reward of cyber criminality and develop a fully functioning cyber counter-attack capability (showing that the UK will "not only defend itself in cyberspace: we will strike back in kind when attacked"). It will also pursue and prosecute offenders internationally.

3. **Develop:** develop the skills and capabilities the UK needs in its economy and society to keep pace with the threat in the future. For example, the UK is creating a virtual network of universities dedicated to technological research.

Taken from Philip Hammond's speech on 1st November 2016, which further explains the three core objectives set out in the Strategy.

The strategy also sets out the various roles Government, businesses and individuals have to play, and signals an increased role for Government in the UK's cyber security. In addition to focussing on the NCSC, the strategy states that the Government will use levers (including the new General Data Protection Regulation) and incentives (for example, supporting start-ups) to drive up cyber standards. It intends to become an early adopter of new technologies, and also promises to ensure that the right regulatory framework is in

place. The strategy acknowledges that regulation should be harmonised with regimes in other jurisdictions, so that UK businesses are not overly burdened with a fragmented approach, although interestingly there is no reference to the EU's new cyber related NIS Directive, which applies in Member States from May 2018.

In part, this increased role for Government is driven by a belief that the previous strategy's reliance on the market to drive the correct behaviours failed to deliver the scale and pace of change required. The report states that while progress has been made in the last five years "too many networks, including in critical sectors, are still insecure. The market is not valuing, and therefore not managing, cyber risk". However, it also places a clear responsibility on businesses to protect themselves and their customers. One of the key strategic outcomes listed in the strategy's headline implementation programme is that "all organisations in the UK, large and small, are effectively managing their cyber risk, supported by high quality advice designed by the NCSC underpinned by the right mix of regulation and incentives."

When launching the strategy, Mr Hammond was also keen to stress that Government cannot be solely responsible for managing cyber risk. He warned (in his speech on 1st November launching the strategy) that, "Chief Executives and Boards must recognise that they have a responsibility to manage cyber risks, just as they would any other operational risk. Similarly, technology companies… must take responsibility for incorporating the best possible security measures in the design of their products."

Comment

The message that cyber is a board issue to be managed as any other business risk issue is not a new one. We have been advising clients on how to incorporate cyber risk management into their governance structures for a number of years. In particular, we encourage our clients to follow our seven key steps to cyber preparedness (see box below) to ensure they are able to mitigate and manage their cyber risk.

However, the report (which is a mixture of aspirational goals, and more detailed measures) suggests that, for now, it does not trust business alone to deliver the required changes in attitudes. The success of the strategy will therefore depend to a large extent on:

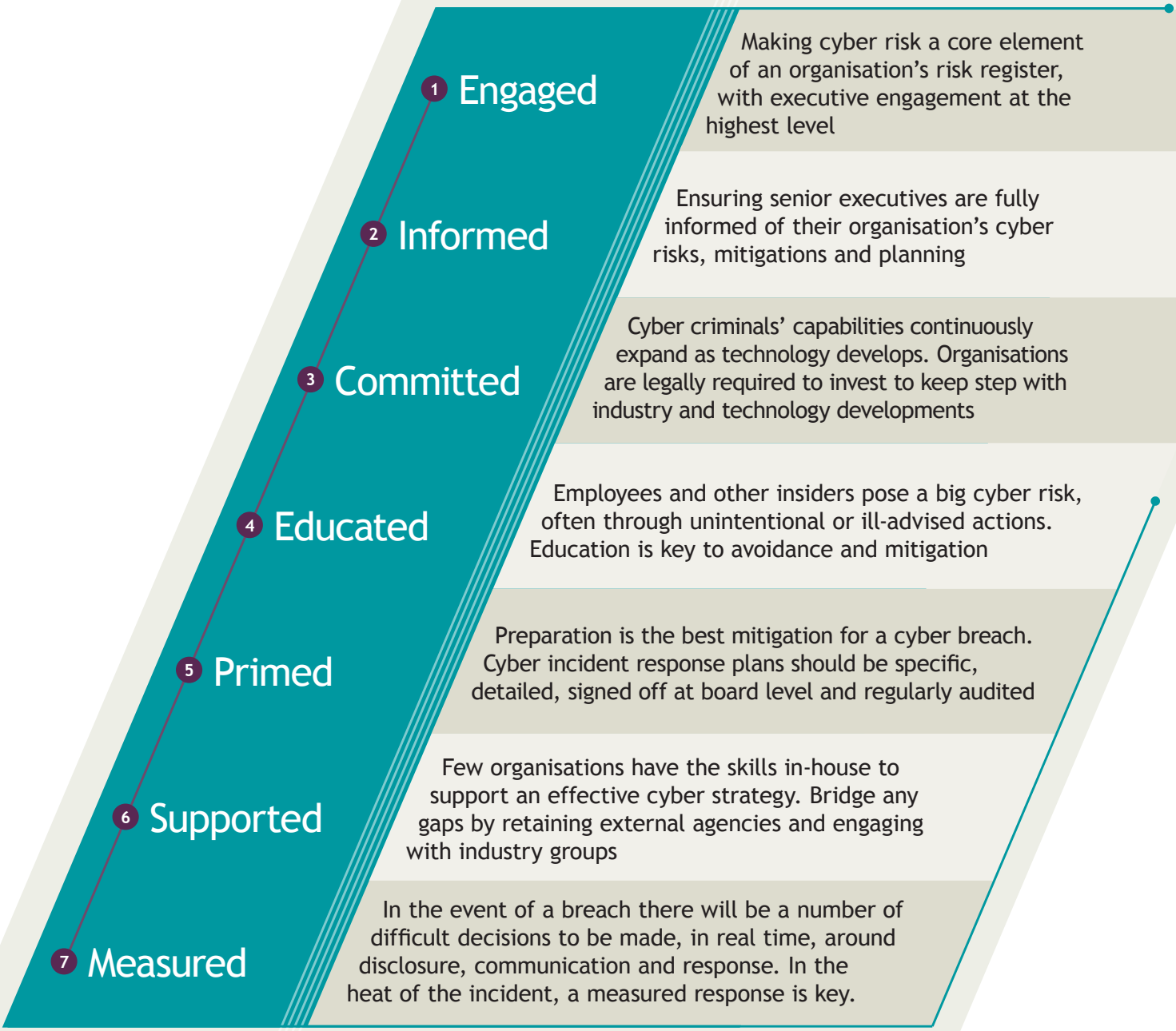
1. How successful the Government is in 'leading by example' (adopting, and requiring in its supply chain, cyber-secure technologies), driving change in the cyber market, and deterring cyber criminals from targeting the UK. We welcome increased engagement by Government, and see support in a national cyber security infrastructure and the cyber market as vital for UK organisation to effectively combat this threat;

2. How businesses prioritise cyber security. In our view larger organisations are increasingly aware of their cyber risk, and that investment is needed to manage this, although this may still not be the case for all businesses. Industry still has a vital role to play, and the strategy clearly states that the Government will work with the private sector (and insurers and others who can influence the market) to ensure businesses and individuals "adopt the behaviours required to stay safe on the internet".

3. What measures (sticks and carrots) the Government will adopt to back-up the aims of the strategy. The strategy report states that the Government "will have measures in place to intervene (where necessary and within the scope of [its] powers) to drive improvements that are in the national interest." We believe that effective guidance and threat information is as important as effective regulation, and will be interested to see what these measures will be, and whether they will involve new legal or regulatory powers.

The cyber solution

We encourage our clients to take 7 key steps to cyber preparedness



Key contacts

This article was written by Paul Mudie and Natalie Donovan of Slaughter and May's Cyber Group.
If you would like further information or advice on any cyber security issues, please contact Paul Mudie, Rob Sumroy, Victoria MacDuff or your usual Slaughter and May contact. We have also produced a series of cyber related publications which may be of interest.

Paul Mudie
T +44 (0)20 7090 3973
E paul.mudie@slaughterandmay.com

Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Victoria MacDuff
T +44 (0)20 7090 3104
E victoria.macduff@slaughterandmay.com

April 2017

OSM0009465_V04