Through The Looking Glass: Alice’s Reflections on Cyber Incident Reporting
October 9th, 2013

In Lewis Carroll’s sequel to Alice In Wonderland, ‘Through The Looking Glass’, Alice contemplates what the world looks like on the other side of the mirror. In the book, there are many reflective themes, drawing on chess, where white is black and black is white, other opposites and time running backwards.

BIS Call For Evidence

BIS recently issued a summary of responses to its Call For Evidence (CFE) on the proposed EU Directive 2013/0027 (COD) (Cyber Directive) on Network and Information Security (NIS). The CFE summary demonstrates that businesses, like Alice, are on one side of the Looking Glass. Their counterparts at the EU Commission are on the other. Each takes a different perspective on how to share incident reporting data to help tackle the cyber threat.

Cyber Directive

In brief, the draft Cyber Directive places a mandatory reporting obligation upon businesses which have suffered an incident. It requires certain businesses to deploy appropriate security measures and to report incidents having a ‘significant’ impact. It is broad in scope and, if adopted, will apply to:

- public administrations;
- providers of critical national infrastructure (CNI); and
- providers of information society services, including social network providers, search engines, app stores, e-commerce platforms and cloud computing and other ‘software as a service’ (SaaS) services.

Please see Pitmans’ previous update on the Cyber Directive and incident reporting here.

Industry remains bewildered by the Cyber Directive’s reflection

In particular, respondents to the BIS CFE who may be affected by the proposals are concerned by:

- duplicative reporting requirements which would place an unnecessary burden on top of existing reporting duties to sector specific regulators;
- conflicts with existing Data Protection regulations;
- how it affects innovation and the development of good cyber security practice; and
- how it may weaken existing voluntary information sharing and trusted exchanges (i.e. mandatory reporting data is unlikely to generate meaningful, genuinely valuable data).

In addition, there is a criticism that those with more sophisticated cyber security and reporting measures may be penalised. Similarly, it was uncertain if confidentiality can be maintained and, ironically, whether the disclosures themselves may remain secure. Finally, there was uncertainty as to how SMEs and smaller organisations are going to be able to meet the requirements imposed by the Cyber Directive.

Banks Remain Strategic Target on Cyber Chess Board
In this context, The Bank of England (BoE) and the Treasury have highlighted the vulnerability of banks and mortgage lenders to the risk of cyber attack. They want board directors (and, specifically, not IT Directors, to draw up plans to address the issue within the next six months (i.e. by end of March 2014). And, it has been revealed from last month’s minutes of the Financial Policy Committee (chaired by Mark Carney, the recent replacement Governor) that The BoE itself will be testing its own resilience.

Cyber War Games

Reminiscent of the 1980s Cold War film, ‘War Games’ where a young computer enthusiast unwittingly hacks into the US government’s WOPR (War Operation Planned Response), UK financial services institutions and payment supplierS will be tested by scheduled resilience tests. These tests will be designed to measure their ability to respond to cyber-attacks. The mock cyber war games is to take place in mid-November. Given it is a scheduled drill, it is hoped that future exercises will be run without warning or notice (given that this is likely to be the case with most ‘real life’ simulations). The Operation is called Waking Shark 2 (possibly, the next catchy title for the next blockbuster cyber film, following the success of ‘The Social Network’? Possibly not).

If you would like advice or assistance as to how to minimise the impact of the Cyber Directive or simply to help us manage risk in your organisation, please contact Pitmans’ Cyber Risk Management or Information Technology teams.

Philip James
Partner & Joint Head of Technology
T: 0207 634 4655
E: pjames@pitmans.com

Posted by Pitmans | Filed in Cyber Risk Management, Data Privacy, Information Technology, Technology
No Comments »