pitmans
MAKING IT HUMANLY POSSIBLE

UK Businesses and the Cyber Threat

Over recent weeks there has been a surge of press and public interest in the cyber threat to the UK. The stuxnet worm attack on Iran initially caught the public imagination, but the focus has been sustained by Government comments highlighting this area as requiring major attention and expenditure over coming years. The fact that this public debate has been going on alongside the Strategic Defence and Security Review, and the more general Spending Review, is no coincidence, given the competition for funds. But it is clear that this is a major area of threat to government, the national infrastructure, companies and individuals which has been neglected until recently.

There is no need to reiterate here the wide-ranging nature of the threat from cyber attack, whether originating with a lone hacker with limited intent, or at the opposite end of the scale the suggestion that some national governments have been involved in attacking parts of other nations' IT infrastructure. It is important that in the UK we appreciate the significance of this threat and guard against it, and as individuals we obtain what protection we can against identity fraud and similar attacks via our home computers or similar networked devices. UK Government may have been a little slow to turn its full resources to the cyber threat to our infrastructure and military defences, but recent initiatives including the establishment of the Office of Cyber Security and the Cyber Security Operations Centre, and more recently the confirmation in the strategic and spending review that cyber defence will receive significant funding, show that it is now well up the agenda and being addressed. Equally, individuals may have varying levels of appreciation of their exposure via home electronics but at least this is an individual threat for the most part rather than systemic.

What is more difficult to be sure of is the extent to which UK companies are doing what they need to in this context. As well as it being a governmental and individual responsibility, protection from cyber attack is a corporate responsibility and failure to grapple with that could have significance for companies around the UK, both in terms of their legal duties and the practical significance of a major interruption in their ability to trade normally resulting from cyber attack.

We are fortunate in this country that our role in the development of information technology over the last few decades, both for corporate and consumer use, means that we have a range of companies which can provide or supplement the ICT systems required to protect the country and its national infrastructure against cyber threats. It is not those companies that are likely to be the problem here. It is companies in other sectors, financial services, utilities, transport and energy particularly that need to ensure they have focused on all aspects of the cyber attack risk. Many of them will be well prepared, but others will not have realised the extent of the risks they are exposed to.

This is unlikely to be a problem that UK Government will be able to deal with alone, and some of the largest international ICT providers are fully engaged in partnering with

governments and industry in this context to develop the protective infrastructure. There will need to be various lines of defence. At a national level it is clear that there are increasing efforts to identify generic threats that are appearing in the form of malicious software, but companies from multinationals to smaller local enterprises will be involved in the process of developing the protective programmes to enable companies and individuals to safeguard their ICT. And it is for all companies in whatever sectors to ensure that they are using the most up to date protective systems.

For companies, failure to do so will mean vulnerability across a whole range of activities. If as individuals we are realising how much of our lives are conducted online, through the web or the telecoms networks, then this is even more the case for companies delivering essential goods and services to the UK and internationally. If the Iranian nuclear industry can be specifically targeted and rendered inoperable as a result of an attack on its ICT systems, then this can happen to any UK company's functions unless adequately protected.

For company boards and management, this is a matter of immediate concern. Many UK companies will have statutory duties to deliver services, and the inability to do so is likely to result in costs (over and above the simple loss of revenues) in the nature of damages or indemnity obligations which could be crippling. Force majeure provisions in contracts may in some circumstances come to their assistance but the process of arguing that through would itself be costly and potentially damaging. Turning to the financial services industry, it is immediately obvious how damaging to a major bank it would be if widespread fraud, or collapse of operations, resulted from a significant cyber attack. As well as the potentially catastrophic effect on the normal function of the bank in terms of borrowing to meet its funding needs (we have seen in recent years how much all banks rely on the inter-bank market) there is the reputational damage that would flow from even a less systemic problem.

Public listed companies have duties under their regulatory regime to ensure their systems are robust, and in the specific financial services arena the FSA also imposes further layers of obligation. There are also duties arising for all companies to their employees in terms of providing a safe working environment in the widest sense, and to customers in terms of the data protection. All of these obligations may come into the equation in the event of a major cyber penetration which brings operations and normal functioning to a halt. The threat is that fundamental.

So, individual directors need to ensure they are taking the best advice from ICT providers about the nature of current threats and the ways to protect against them, and from their other advisers on how to ensure their internal governance structures are robust (and clearly set out) so as to manage these risks. We may find as a result that corporate life becomes less accommodating for employees in terms of free and easy access to external connectivity over time. It already has for those engaged in defence related contracting in the UK, where the MOD's information assurance policies impact on all suppliers. The effectiveness of protective systems may improve so as to help management in this area (but so may the cost) and it is essential that the effectiveness of that protection is kept under regular review in the context of general risk management planning.

However it is achieved, companies need to be sure they are doing everything reasonably practicable to protect themselves, and by extension their ability to provide continuity of service to their customers and the public at large. Failure to do so will not only expose

them to the cyber threat itself but to the potentially serious knock-on liabilities and other consequential effects, whether for the organisation as a whole, or for the individuals responsible for those failures.

Andrew Peddie
apeddie@pitmans.com
+44 (0) 118 957 0321