Cyber crime continues to rise up the board agenda as directors begin to recognise their full exposure to attacks. KPMG Information Protection Partner, Stephen Bonner, tells Criticaleye how to minimise the dangers of doing business in a digital world.

Seven Ways to Beat Cyber Crime

With many sectors struggling in the recession, cyber crime seemingly bucks the trend as a shady and subterranean growth industry. Boards are slowly waking up to the threat and understanding the damage that can be inflicted on operations and reputation if a business fails to create the appropriate defences and risk-management systems.

A report published at WEIS (Workshop on the Economics of Information Security), exploring the cost of tackling cyber crime, estimates that defence costs, this year alone, were in the region of $500 million. Added to the costs of cyber theft and fraud, lost intellectual property (IP) and reputational damage (which today spreads into the billions of pounds annually), the enormous outlay of keeping pace with the evolving threat is a bitter pill for boards to swallow.

Even so, as can be seen over the following pages, there are effective approaches that can help minimise the cost and the risk presented by cyber crime...

Know Your Enemy

Boards need to be aware of which threats they are up against in the digital space. There are four separate risk areas, with different capabilities, targets and effective controls against them:

- Organised crime which is primarily motivated by stealing money
- Nation state-driven attacks, which often seek IP and insider information
- Hacktivists, who are driven by a political agenda
- ‘Insiders’ – these pose a rising threat in a downturn and are often disgruntled or alienated staff with a personal vendetta.

Although all different in terms of scope and approach, each of these threats offers a substantial risk to the security of every business. While some businesses will be more exposed to certain dangers than others, successful defences will have to strike a balance, as ignoring any of the above would be a mistake.

Be On the Front Foot

It's a simple fact that acting to secure an organisation after one breach, or even more, is just not good enough. Being proactive is the name of the game and it is too late to just heavily invest in an area exposed by the last incident.

Thankfully, cyber crime has climbed the board agenda. There have been vocal statements made by both MI5 and the FBI this year.
about the scale of the threat, and with the private sector making in-roads into critical government infrastructure, both in the UK and in the US, it isn’t difficult to see why politicians are keeping a close eye on whether boards are effectively securing the data for both their businesses and their clients.

Delegate at Your Peril

Allowing IT to dictate your cyber strategy is to delegate responsibility for a business’s whole security, as well as that of every customer and supplier. It is a cardinal sin and for boards it is a dereliction of duty.

While many successful cyber risk frameworks begin within IT, as they gain momentum and scope they usually take responsibility for broader issues like privacy, records management and data quality. At that point, they become a governance function that needs to be separate from IT if they are to provide oversight of it – this risk-type function should report to the board.

The most effective risk functions are those that can take on the greater mandate without necessarily growing in scale. Here, talent is key and HR can ensure that cyber risk teams are stocked up with flexible people who can build relationships across audit, IT and central business teams.

Any cyber risk strategy first needs to invest in updating staff defences

While IT certainly brings an understanding of the most technical challenges posed by cyber crime, those able to drive change throughout the organisation must be highly competent generalists, leaders and communicators and not purely technical experts.

Find the Weak Links

There’s an increasing awareness among organisations that no one is alone in this space. As convergence continues apace across a range of industries, both supply chains and customers are inextricably tied to the databases of nearly every business. Improving the general standards of data security has obvious benefits and organisations are very clearly stronger together. Although sharing the means to defend against cyber crime has undoubted benefits, data sharing brings with it its own problems. In gathering large volumes of data to get insight into customer behaviour, there are obvious risks to the customer should that personal information be leaked, as well as businesses facing the worrying possibility of corrupted or edited records generating incorrect and misleading business insights.

Moreover, as connectivity between ‘work’ and personal devices increases, the use of third-party apps to process proprietary data is becoming more widespread. For risk managers, that poses the question of how to enable staff to be effective and productive with the latest technology, without private data leaking into the public domain.

Be Brave

There is a sense that the sheer scale of a business’s involvement in the digital space makes many of these issues inevitable and impossible to avoid, but with a tried-and-tested response plan, boards can ensure that they are comfortable with both standard operating procedures as well as what happens on those rarer occasions that demand decisions are referred upwards.

The landscape is constantly changing as new technology evolves. While many new risks will emerge, boards have to ensure that a safe approach doesn’t stop them adopting the latest technology to remain competitive in the future.

© CriticalEye 2012

Stephen Bonner
Partner
KPMG

Stephen is a Partner in the Information Protection team at KPMG where he leads a team focused on Financial Services. Before KPMG he was Group Head of Information Risk Management at Barclays. He was inducted into the InfoSec ‘Hall of Fame’ in 2010 and was number 1 on the SC/ISC2 ‘Most Influential 2010’ list.

Contact Stephen through www.criticaleye.net