RISK DOCTOR PARTNERSHIP BRIEFING

MANAGING CYBERCRIME RISK

© May 2014, Ben Rendle

ben.rendle@rioscaconsulting.co.uk

Cybercrime is a rapidly growing threat to the global economy. But it is not well-defined, and it is often confused with cyber-warfare or cyber-terrorism. Risk professionals need to understand cybercrime and its links to risk management, as we can provide valuable assistance in countering this significant threat to business and society.

Some risk professionals think cybercrime is only relevant to technical people and that it should be tackled by the IT departments. But cybercrime poses a significant risk to organisations because it affects their ability to achieve strategic and operational objectives. Unfortunately many businesses don’t know what cybercrime looks like, how likely they are to be affected, what the extent of the impact might be, or how best to manage it.

Cybercrime can affect an organisation in many different ways, including:

- online theft or fraud
- identity theft
- extortion
- theft of customer data
- theft of intellectual property
- industrial espionage

Exposure to cybercrime is related to the level of online activities undertaken by an organisation, including the scope of their online presence, the extent to which valuable assets and information are stored online, the strength of online security, and the degree of risk awareness in the organisational culture.

To manage the risk of cybercrime, we must first identify the level of our online activities, and determine which assets and activities might be affected by cybercrime. Then we can begin to identify, assess and manage our cybercrime risks. The following steps will be helpful:

- **Clearly understand and define organisational objectives for online activities**. Recognise the different and specific online environments of our stakeholders, and assess their appetites for online risk.
- **Address cultural as well as technical factors**. These include cultural barriers, communication difficulties, and the effects of bias on perceptions of cybercrime risk.
- **Recognise internal as well as external cybercriminal threats.** Insider threats can arise from employee errors, accidental data loss, or malicious leaks of sensitive corporate data. External threats might come from hackers, pressure groups, competitors or even hostile foreign governments, as well as viruses, worms, Trojan horses etc.
- **Establish ownership, accountability and incentives to address cybercrime risks.** All senior staff should be accountable for managing cybercrime risk in their area of responsibility, and we should challenge stakeholders who view it as “not their problem”.
- **Manage cybercrime risks within an Enterprise Risk Management (ERM) framework.** Cybercrime risks can affect the wider enterprise in areas such as reputation, business continuity and knock-on effect to subsidiaries and suppliers, so it needs to be tackled in a coherent way as part of our overall response to risk.
- **Develop a global perspective on cybercrime risk impacts.** Many organisations depend on overseas economies for trade, exports and wealth generation, and this exposes them to overseas cybercrime which cannot be ignored.

As risk professionals, we need to include cybercrime in our thinking and practice, so that we can offer practical targeted advice to our organisations to reduce the threat and protect our business.

To provide feedback on this Briefing Note, or for more details on how to develop effective risk management, contact the Risk Doctor (***info@risk-doctor.com***), or visit the Risk Doctor website (***www.risk-doctor.com***).