Group Risk Consulting Ltd.
Governance. Risk. Compliance.

Cyber Risk Management

Cyber-attacks are increasing in scope and sophistication at a time when businesses are moving their key assets and systems to a digital sphere. Increasingly, company assets are changing in nature from being tangible to intangible. This makes them more difficult to manage, protect and insure.

The economic impact of cyber-crime was estimated to be $600 bln (or 1% of global GDP) a year in 2018. Up from $445 bln in 2014.

The UK government has classified cyber security as a 'Tier 1' threat alongside international terrorism.

Cyber risk no longer is the sole responsibility of the CIO and CRO, but should be owned by the whole senior management team. Company directors need to understand that failure to maintain adequate cyber security may be subject to claims by stakeholders and affected individuals in addition to increasingly severe regulatory fines. The 2018 Corporate Governance Code clearly states senior management responsibilities for managing cyber risk, a 'must read for all directors!

Effective management of cyber risk, does not mean that a company must prove immunity from cyber breaches, as this would be impossible. Rather, it should be able to demonstrate a detailed understanding of its cyber risk profile, total risk exposure value and how the company manages this responsibly and sustainably with reasonable care, skill and diligence.

Can you (or the management team) confidently answer the following questions?

- What are the company's key assets, where are these located and how are they protected?
- How are management informed about the current level of exposure, potential business impact and remediation action status of cyber risks?
- How does your cyber risk program meet key regulatory requirements / guidelines and how often is this reviewed?
- How many and what type of cyber related incidents do you detect in a normal week and what are the senior management reporting thresholds?
- How much did cyber risk events / impacts cost in the last year?
- How comprehensive is your cyber risk incident response plan and when was it last tested?

If you have trouble answering some of these questions you may need to enhance your cyber risk management capability. If so, Group Risk Consulting can help you:

- Gain a much better understanding of your cyber risk profile, by conducting a cyber risk assessment exercise that is tailored to your company and industry
- Identify the gaps in your existing cyber risk management programme
- Understand your regulatory compliance requirements
- Assess your ability to respond and recover from a cyber risk incident
- Determine if you have the opportunity to insure any identified exposures
- Identify any management and, or stakeholder reporting requirements.

GRC

Some key benefits of conducting such a review include:

- Increased levels of cyber risk resilience
- Reduced probability of loss
- Greater confidence in your existing response and recovery plans
- Increased assurance that key suppliers/partners understand their role in your cyber risk management programme
- More confident board and senior management team and confident workforce
- Identification of redundant or inefficient processes
- Greater levels of regulatory compliance
- Potential cost savings
- Optimised insurance programme
- More complete enterprise risk management framework
- Improved levels of corporate governance
- More confident suppliers / partners and investors
- More robust and sustainable organisation.

For more information in relation to how to manage or insure the risks of reputation damage, please contact:

Michael Porteous
Managing Director, Group Risk Consulting Ltd.
Email: michael.porteous@grouprisk consulting.com
Tel: +44(0)7710194472