

# Sydney Charles Insurance Advisers Limited

## Are Your Management Fees Secure in the Event of a Cyber Attack?

May 2017



Cyber insurance should no longer be seen as optional but an essential part of a fund manager's risk management strategy.

Most traditional insurance policies are insufficient to effectively respond to cyber threats, which is why Sydney Charles offers specialist cover that includes loss of management fees.

While appropriate protection will not stop a cyber-attack, it may prove to be the decisive factor in ensuring a swift recovery and a limited impact on sales, revenue, customer trust and reputation.

### Why is Cyber Coverage Needed?

Businesses around the world continue to take stock in the wake of the WannaCry ransomware attacks, which hit more than 200,000 computers in 150 countries.

As a specialist insurance broker, Sydney Charles can consult with fund managers to perform a cyber risk assessment and gap analysis to identify these cyber risks and exposures, and we can ensure appropriate cover and protection.

Most Asset Management companies would already have in place the following types of coverage, each of which exclude cyber risks:

**Professional Indemnity:** These policies may not respond to cyber intrusion and the resulting losses or damages. Business interruption due to system failures (no physical cause) and business interruption triggered by a cyber attack are unlikely to be covered with specific exclusions around breaches of employee information.

**Crime:** Crime policies directly exclude indirect loss meaning any business interruption claim would not be covered.

### What Does Specialist Cyber Coverage Include?

**Loss of Management Fees:** The company receives a redemption from an investor, or similar request by a fund, following a business interruption. Cover is provided for the value of the management fees the company would have earned for a period of one year (this does not include any performance fee, carried interest income, or similar performance based income).



**Increased Cost of Working:** Additional operating costs including services, employing contract staff and overtime costs as a result of a business interruption event.

**Crisis Response:** 1st party direct loss of business due to an interruption of business dependent systems to include:

- Contracting specialists and overtime costs of employees working to identify and resolve a system event
- Expenses incurred as a result of material damage to the Insured's brand and reputation
- Legal, public relations, advertising and any other reasonably incurred expenses to comply with a requirement by an official regulator or consumer ombudsman to notify clients of a system event

**Data and Software Restoration:** Replace hardware affected by a security event to include the cost of:

- Employing contract staff or overtime cost of employees to repair, restore, re-collect, or reconstruct the Company's affected data or software applications
- Licenses to re-install any affected software applications

**Privacy Breach Management:** Costs and expenses in executing a strategy for responding to a privacy event.

**Security & Privacy Liability:** Coverage for defence costs and damages for third party claims arising out of a network or privacy event.

**Cyber Extortion:** Costs and expenses to include any ransom paid as a result of an extortion demand.

If the above would be of interest all we will require is the following information regarding investors and fee structures:

1. Number of individual investors
2. Average investor value
3. Average management fee
4. Names of fund administrators
5. Description of contractual risk transfer

**Darren Le Couvey**  
Insurance Manager

Tel: +44 (0)1481 739970

Email: [darren.lecouvey@sydneycharles.co.uk](mailto:darren.lecouvey@sydneycharles.co.uk)



[www.sydneycharles.co.uk](http://www.sydneycharles.co.uk)