Remarks of Simon Lewis at launch of the ICAEW report, ‘Cyber-Security in Corporate Finance’

As the Minister starkly puts it in his foreword, Sir Iain Lobban, the Director of GCHQ, reports that Britain is experiencing industrial espionage on an industrial scale. AFME supports the government’s efforts to publicly highlight this huge risk and, in particular, to ensure that the directors and senior executives of companies take responsibility for dealing proactively with the threat.

AFME believes that cybersecurity is not a responsibility that should be delegated to IT and information security executives alone. We believe that, in financial institutions, the management of this risk should be reviewed at the level of its board’s risk committee or equivalent board committee.

We are pleased to have participated in this ICAEW-led task force, which has produced this reference guide for all those involved in various capacities in the corporate finance sector. The guide presents a number of possible approaches to managing various aspects of cyber risks in a way that recognizes the diversity of the firms involved, their respective roles, and the relative complexity of different business models. It recognizes the need for flexibility in selecting and applying the approaches presented.

Focused, continuous vigilance is a key message to be taken from this timely report. Cyber intrusions may occur at any of the stages of a corporate finance transaction. This is because it is widely understood that sensitive information will be exchanged between authorised parties at each stage of a deal or potential deal. Given the number of people involved in every stage of the transaction, and the large volumes of information shared, corporate finance transactions pose greater risks than business-as-usual transactions.

The task force has also met with AFME’s Corporate Finance Committee, comprising senior bankers from 12 leading investment banks. In addition to providing input to this guide, the committee has decided to issue a new policy recommendation.

AFME members who are engaging in corporate finance activities should include cyber-risk in due diligence checklists and, where appropriate, discuss cyber-risk with responsible board members or senior executives of the companies involved. This policy is published on our website on 16.01.14.

We think this is an important and timely step for our members to take. What is at risk here is trust in the financial system in which corporate finance plays such a crucial part.