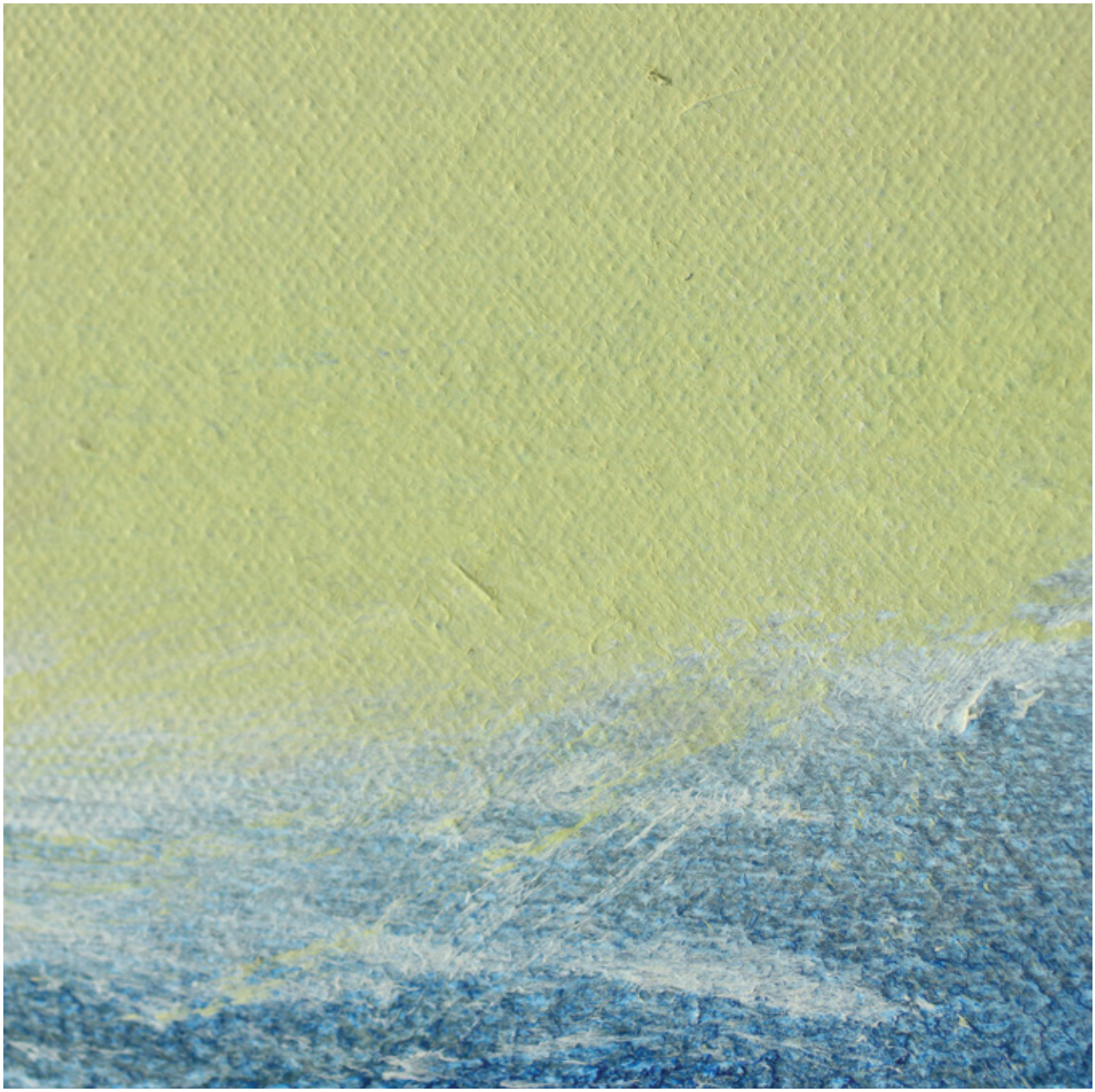
Detail from Sea Hook by Trevor Bell

CONTENTS

SLAUGHTER AND MAY

Quarterly Update

APRIL 2014



Detail from Early Morning by Trevor Bell

Cyber security – a real world issue

Cyber security is now a Board level issue for many companies, and one that lawyers advising the Board must understand. But what is a cyber attack? Who are the cyber criminals? And what are businesses, and the Government, doing to protect against this increasing threat?

'INDUSTRIAL ESPIONAGE ON AN INDUSTRIAL SCALE'

Cyber security has recently attracted the attention of the world's governments and media alike. High profile security breaches at brands like Sony and Adobe have attracted global headlines, as have the Prism revelations and rising diplomatic tensions over alleged state-backed hacking.

Closer to home, the Director of GCHQ has declared that Britain is experiencing 'industrial espionage on an industrial scale', and UK Government statistics state that 93% of large corporations reported a cyber breach last year. [1]

Organisations are therefore becoming increasingly aware of the risks associated with cyber attacks. Cyber security is now a Board level issue for many, and one those advising the Board must understand.

In this article we go back to basics: what is a cyber attack, who are the cyber criminals and when are companies most at risk? We also look at some of the steps companies can take to protect against cyber threats and focus on recent guidance issued on "Cyber Security in Corporate Finance". Finally, we highlight what the UK and EU legislators are doing to try to tackle this 'Tier One' threat.[2]

CYBER ATTACKS: WHAT ARE THEY AND WHO ARE THE PERPETRATORS?

The term 'cyber attack' is very broad. It is currently used to describe many different types of attacks on computers and computer-based equipment and information through the use of other computers – the aim being to compromise the integrity, availability or confidentiality of those computers, equipment and/or information.

The method of attack varies greatly, as does the source of the threat and aims of the attacker. Common attacks range from denial of service attacks which target a website or server, to phishing and spear phishing attacks which target individuals *(see the Glossary below for more information)*.

Cyber criminals come in many shapes and sizes. Some are financially motivated, while others have commercial, political, ideological or personal drivers.

1 www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace

2 The Government has categorised cyber attacks as a 'Tier One' threat to our national security, alongside international terrorism – https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty

CYBER ATTACK: WHY, WHO AND WHAT?				
Why?	**Business** Aim: to profit from the attack		**Ideological** Aim: to cause disruption and/or harm	
Who?	**Financial** Criminals	**Commercial** Unscrupulous competitors Governments	**Political** Hacktivists Terrorists Governments	**Personal** Disgruntled employees Personal grudge Hackers
What?	Anything that can be sold, or otherwise used to make money such as: (i) commercial secrets which can be sold; (ii) personal secrets which can be used to blackmail; (iii) financial details (e.g. credit card details or bank account passwords); or (iv) information affecting the share price of a company	Commercial information or trade secrets which can be used by competitors or nation-states seeking advantages for state-sponsored industries Could include cutting edge IP, business/strategy plans, confidential negotiation positions, prices, customer details	Anything that can: (i) cause damage and/or disruption to a country's critical infrastructure, security or business interests; (ii) attract publicity or obtain information to support a political agenda (e.g. animal testing); or (iii) provide information on the activities of another state (government espionage)	Anything that can: (i) cause damage, destruction or embarrassment (e.g. damage to an individual, company profits or company reputation); or (ii) increase a hacker's reputation (e.g. some hackers gain notoriety from penetrating 'secure' systems). Young hackers (sometimes called script jockeys) can easily access 'hacking kits' online

WHEN ARE COMPANIES MOST AT RISK?

While it may be difficult to predict if/when a company will suffer a cyber attack, certain factors can increase the risks, for example:

- *Operating in a high-risk sector*
  The UK Government has identified certain sectors which relate to the provision of 'essential services' as being particularly at risk from cyber attacks. An attack on an organisation in the health, energy, transport or finance sector could cause significant disruption to the country, making them ideal targets for a politically or ideologically motivated hacker. Similarly, at an EU level, the proposed Network and Information Security Directive *(see upcoming EU legislation in the Legislation Tracker below for further detail)* identifies

certain sectors as 'market operators' who would need to adopt risk management practices and report major security incidents.

- *Developing new products/technologies or focussing on R&D (e.g. pharmaceutical or manufacturing companies)*
  Intellectual property and information on new product or technology developments are extremely valuable company assets. By compromising a computer system or targeting a key employee to steal this information, an unscrupulous competitor can beat a rival to market or undercut the developer's price. Although for confidentiality reasons many of these attacks do not reach the public domain, there have been some published examples – for example an email-based cyber attack targeting a research director led to a biotech company having its research on a new pharmaceutical product stolen. This enabled a foreign competitor to release a cheaper product onto the UK market before the UK company, damaging the company's profits and ability to secure funding for further R&D.

- *Engaging in corporate finance transactions*
  When a company engages in a corporate finance transaction, such as M&A activity or a refinancing exercise, it is common for large amounts of important and highly sensitive information to be collected together and shared between multiple parties and advisors. This increases the risk of a cyber attack for the companies involved, along with their advisors, investors and/or financiers. In addition, the transaction itself may increase the cyber risk as a company may acquire a target which has already been compromised by a cyber attack, or which has weaker systems making it more vulnerable to attack. In our Cyber Security Focus below, we look at the recent "Cyber Security in Corporate Finance" guidance published by the Institute of Chartered Accountants of England and Wales, with support from the Government, and discuss some of the practical steps a company can take when undertaking a corporate finance transaction.

- *Dealing with state-related counterparts in jurisdictions with a higher incidence of cyber attacks*
  While commentators estimate that many states around the world are involved in cyber espionage, a number of countries (for example China and Russia) have attracted particular media attention for alleged hacking of (often Western) organisations. Unscrupulous competitors and nation states wishing to steal information or support state-backed organisations, may use cyber attacks to obtain confidential plans, negotiation positions, trade secrets and/or intellectual property.

WHAT CAN YOU DO TO REDUCE YOUR RISK?

Cyber attacks are increasing both in terms of volume and sophistication. It is therefore impossible to eradicate the risks. However, many online attacks can be detected or (ideally) prevented with basic security practices.

There are a number of practical steps you can take, and guidance you can follow, to help protect against cyber crime. This includes managing cyber risk within your corporate governance structure as a business rather than technology risk – i.e. proactive planning and management by the Board, with senior management leading implementation of an information risk management regime and reassurance through the corporate governance process.

PLAN:

- Protecting your information is a Board responsibility: Government guidance[3] confirms that pro-active management of the cyber risk at Board level is critical. But does the Board have the full picture? Have they identified and agreed what are the key information assets, the likely cyber risks and the company's appetite for risk? Do they understand the impact on the company's reputation, share price or ability to survive if: (i) sensitive internal or customer information were to be stolen or compromised; or (ii) your online services were to be disrupted for a sustained period? Also, has responsibility for the cyber risk been appropriately allocated (e.g. is it on the risk register) and is the Board kept up to date with developments (for example, does the CIO provide regular intelligence updates on the latest threats and methods of attack)?

- Is your business subject to any particular legal and/or compliance issues? The data protection regime requires that adequate security measures are in place whenever an organisation is dealing with personal data, and certain sectors (for example, the financial services sector) have additional regulatory requirements. Also, different jurisdictions may have different legal requirements around key security techniques such as encryption (for example, some states prohibit encryption unless the encryption keys are provided to certain authorities). Multiple jurisdictions can also complicate matters as conflicting laws and regulations may make it difficult for multi-national organisations to plan a single international strategy.

- Have you considered how you would respond to an attack? Could you continue doing business? Would you need to notify anyone or obtain the help of any third parties? While good cyber hygiene practices will go a long way to protecting vital IT systems, they can never eradicate the problem altogether. An important part of effective cyber security is considering what should be done if there is a cyber attack.

IMPLEMENT:

- Many organisations will already have some form of risk management regime. The first step is often therefore to ensure that this now also covers information and cyber risk. Once you have established an information risk management regime and defined your attitude and approach to risk management, it is important to communicate this throughout your organisation.

- Do you have appropriate security policies and controls in place to protect your IT systems, equipment and information? The Government has produced guidance (10 steps to Cyber Security[4]) on some of the measures organisations should take into account, from home and mobile working, to network security and user education and awareness. Educating staff is particularly important: users are often the weakest link in the security chain and targeting an employee (for example, encouraging them to open an email with malicious content) can be cheaper and more effective than mounting a technical attack.

- As many organisations now have complex technology supply chains, or outsource their IT arrangements, any policies and controls should also cover these supply arrangements. You may also want to review these contracts to see what contractual obligations and security provisions the suppliers have in place, and whether any amendments are required.

- Are you engaging in regular information sharing with other companies in your sector, regulators and (where appropriate) the relevant authorities? By encouraging

[3] See our List of Useful Resources section of the Focus (below) for more information on guidance for boards and small businesses

[4] See our List of Useful Resources section of the Focus (below) for more information

technical staff to share information with other companies in your sector, you can learn from others, benchmark and help identify emerging threats. Also, one of the central elements of Government guidance and upcoming EU legislation is to encourage greater co-operation and information sharing between companies (particularly the essential services), their regulators and the relevant authorities.

- Do you follow best practice when disposing of IT assets? Basic IT security and data protection compliance recognises that it can be hard to completely remove information from IT assets that are no longer required, and the Information Commissioner (the UK's data protection regulator) has published guidance on this from a data protection angle.

- Does your incident management plan include provisions on what to do if you do suffer an attack? For example, it should consider issues such as containment of the attack (e.g. through network isolation), your PR response if the attack enters the public domain, your communications protocol (knowing your systems may be compromised, how will you communicate internally regarding any investigation?), notification of enforcement authorities and interested parties, protection of intellectual property and the appropriate steps to resume business as usual (including how disaster recovery plans can provide emergency IT provisions where necessary). You should not only consider the immediate impact that a cyber attack will have on your ability to run your business, but also the effect on your share price and longer-term reputation.

- Given that some cyber attacks may lead to litigation or regulatory investigations, any plans should also consider how to maintain privilege in relation to appropriate documentation when carrying out an investigation into the attack.

REVIEW:

- It is important to review and test the effectiveness of your controls. Many companies engage in regular penetration testing of their IT systems. Technical staff should also regularly monitor and review network and system logs for indicators of suspicious activity. Larger companies in key sectors have engaged in sector wide cyber security war games. Recently, the financial sector organised a day long simulated attack on its systems in London (dubbed 'Waking Shark II') following a similar test undertaken in 2012 to assess vulnerabilities to cyber attacks during the Olympics. The findings were published earlier this year (5th February 2014) and highlight a number of areas for improvement.[5] The Government, in a recent communiqué from an event entitled 'Strengthening the cyber security of our essential services' has indicated that it intends to work with partners to deliver and participate in similar programs for companies who are in the essential services sector.[6]

- Are you keeping abreast of the latest developments? More importantly, are you acting on any information you receive, whether on emerging threats, or weaknesses in your controls? Cyber security is a developing area of law and a burgeoning industry in its own right. New tools are continually becoming available and new guidance is regularly published. For example, the Government has recently concluded a consultation on organisational standards in cyber security, and is in the process of creating a new standard[7] on basic cyber hygiene. At a European level, the proposed Network and Information Security Directive will particularly impact on organisations

5 http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf

6 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/277525/Communique_-_SoR_FINAL_v1_FEB_2014.pdf

7 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262114/bis-13-1308-call-for-evidence-on-preferred-standard-in-cyber-security-response.pdf

operating in certain critical sectors *(See upcoming EU legislation in the Legislation Tracker below for further detail)* and so it is important that organisations in those sectors prepare for this additional regulation.

- If you do suffer a cyber attack, will you learn from the experience? For example, will you ensure your response includes the removal of any on-going threat (e.g. removing malware), addressing any security gaps identified by the attack and understanding the cause?

'PUT CYBER CRIME ON THE AGENDA, BEFORE IT BECOMES THE AGENDA'[8]

A successful cyber attack could destroy a company's reputation or financial standing. While the majority of cyber attacks will never make the headlines, and some go completely undetected, the threat is growing both in terms of size and sophistication. Lawyers, and the Boards they advise, should therefore take the cyber threats facing them seriously, and ensure that their organisations adopt a corporate governance framework that prioritises cyber security and which can be modified to meet the ever-changing threat. On a more personal note, many cyber attacks target key people within an organisation, and it is therefore equally important that senior executives and the in-house legal teams who advise them understand that, as guardians of the most sensitive corporate information, they themselves are often the focus of the cyber criminal. Ultimately, both corporate and personal vigilance is required to combat the growing cyber threat.

This article was written by Rob Sumroy, Natalie Donovan and Richard McDonnell. Rob is a partner, and Natalie and Richard are lawyers, in the Technology Group at Slaughter and May.

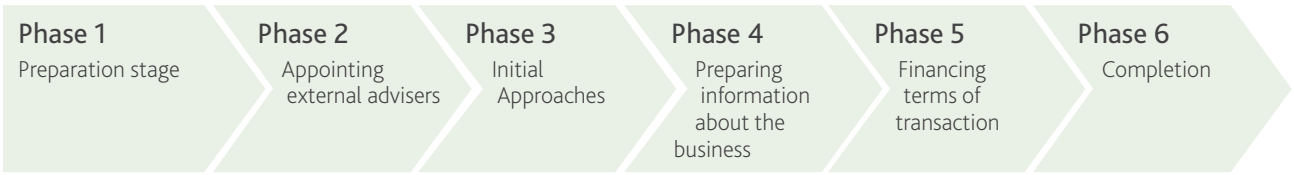
[8] 10 Steps to Cyber Security – page 5

FOCUS: CYBER SECURITY IN CORPORATE FINANCE

Corporate finance transactions are a key part of the business world, and are vital to the wider economy. However, engaging in a corporate finance transaction, whether you are refinancing an existing facility, or acquiring a new company, could make your business more susceptible to a cyber attack. In this focus section we look at the risks involved in the different stages of a corporate finance transaction, and some of the actions that can be taken to help mitigate those risks. In particular, we look at the recent guidance published by the Institute of Chartered Accountants in England and Wales together with the Government and a number of other business organisations on "Cyber-security in corporate finance"[9] (the 'Guidance'). This Guidance aims to raise awareness of the issues involved, and help organisations take the appropriate steps to manage cyber risk as a strategic business, rather than a purely technology, issue.

Why the increased risk?

Corporate finance activity involves multiple parties and the collection and sharing of large volumes of commercially sensitive information. This creates a heightened cyber risk at each phase of the transaction and the Guidance identifies six phases:



For example, at the preparation stage of a business sale/purchase (Phase 1 of the six phases identified above) there is the risk of alerting outsiders to the fact that a transaction may be imminent, while in the latter stages the confidential information collected together and shared as part of the planning and due diligence stages may become the target, along with the negotiation strategies or bid prices of competing bidders. The completion stage itself may also attract attention, as funds are transferred (with the risk of interception) and confidential plans around future strategies are likely to be in place (e.g. potential synergies with the newly acquired business, plans to expand into new markets, or details of how the business will be separated from its previous group). Even following completion, the transaction may still introduce new risks into an organisation, for example newly acquired IT assets may have already been compromised, introducing a weakness into a previously secure system.

[9] http://www.icaew.com/~/media/Files/Technical/Corporate-finance/Corporate-finance-faculty/tecpln12526-cyber-web.pdf

What can you do to manage the risk?

The Guidance discusses the risks, questions to ask and possible actions an organisation can take at each phase of the corporate finance transaction. Some common themes which emerge include:

Information controls	Risk analysis and information gathering	Additional protections
Share information on a need to know basis only – do not provide more information than is necessary to more people than is necessary (operate 'need to know' lists) Keep teams small – for example only a limited number of people need to be involved at Phase 1 Implement procedures to track information flows Hold back particularly sensitive information until later in the transaction Appoint someone to be responsible for looking after information flows/information security in your organisation	Understand your risk profile at each phase – is there anything about the deal which increases the risk (sector, jurisdiction, additional regulatory obligations etc.)? Has the risk profile changed? Identify which information is particularly sensitive If receiving information, ask the party providing it to identify which information is particularly sensitive Use any expertise you have within the organisation – e.g. do you have a security expert who could provide additional help? Ask other parties involved to divulge any increased risks of which they may be aware Include cyber security questions (such as asking what standards the other parties comply with) in the due diligence process Consider/plan what would happen at each stage if a cyber attack were to occur	Ensure people within your team are cyber aware (e.g. do they know to use social media carefully) and understand any deal-specific risks Check you have sufficient measures and procedures in place Consider whether separate IT systems and people may be required where the transaction is particularly sensitive, and check the security credentials of the parties involved (including advisors and data room providers) Monitor access to information and treat particularly sensitive information differently (e.g. more restrictive access, keep information off-line) Ensure appropriate confidentiality and information sharing/use contracts are in place Seek cyber security assurances as part of the due diligence and warranty process Check any systems/assets acquired during the transaction are not already compromised and update your policies and procedures if required

While it is important that both parties keep information secure, each party will also have its own particular priorities. Buyers will want to carry out sufficient due diligence on the cyber threat of any potential target, while sellers will want to ensure that the value of that target is not compromised by any cyber threat or incident. The Guidance therefore highlights how important it is for all organisations involved to build the issue of 'cyber security' into their transaction processes. It is also an indication of how the 'cyber risk' is moving up the UK's corporate finance risk agenda, following countries like the US where the SEC's Division of Corporation Finance published guidance in October 2011 indicating the importance, in its view, of disclosure obligations relating to cyber security risks and cyber incidents.[10] Finally, it is a reminder more generally that "all businesses involved in corporate finance need therefore to be aware of these cyber risks, and of what they can do to help protect their data, their clients and their reputation."[11]

LIST OF USEFUL RESOURCES

Resource Title and Date	Aim
Guidance: Cyber Risk Management – a Board Level Responsibility https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf 5 September 2012	Contains key questions for CEOs and Boards as well as those advising them
Guidance: 10 Steps to Cyber Security https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility 5 September 2012	Contains cyber security information and advice for 10 critical areas (including home and mobile working, network security and incident management), covering both technical and process/cultural areas
Guidance: Small Business Cyber Security Guidance https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf 23 April 2013	Straightforward guidance for small businesses to improve their cyber hygiene
Guidance: Cyber Streetwise Campaign https://www.cyberstreetwise.com/ 13 January 2014	Campaign aimed at individuals which encourages the following cyber behaviours: (i) using strong, memorable passwords; (ii) installing anti-virus software; (iii) downloading patches when prompted; (iv) using privacy settings on social media; and (v) shopping safely online

[10] see http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[11] David Willets, Minister of State for Universities and Science: Cyber Security in Corporate Finance foreword.

Guidance: Cyber Security in Corporate Finance http://www.icaew.com/~/media/Files/Technical/Corporate-finance/Corporate-finance-faculty/tecpln12526-cyber-web.pdf 16 January 2014	Aims to raise awareness of the cyber risks and issues involved in the different phases of various corporate finance transactions, and help organisations take the appropriate steps to manage the cyber risk

Cyber security is a hot topic for legislators in both London and Brussels. Although existing legislation on areas such as data protection and computer misuse touch on cyber security, the general consensus seems to be that more specific regulation is required. Below we set out some of the particular initiatives that are currently underway:

CURRENT POLICIES AND LEGISLATION

Name and date of legislation	Aim
UK	
Government policy: Keeping the UK safe in cyber space 25 November 2011	To prevent cybercrime and make the UK a safer place to do business, the Government's Strategic Defence and Security Review has allocated £650 million over four years to establish a new National Cyber Security Programme, to: (i) set up a National Cyber Crime Unit (bringing together the Police eCrime Unit and SOCA); (ii) provide advice to businesses; (iii) build a cyber information sharing partnership with business to allow the Government and industry to exchange information on cyber threats in a trusted environment; (iv) create a joint Cyber Growth Partnership with Intellect (the technology industry body) to increase understanding of the UK cyber security issue; and (v) introduce "Action Fraud", a single reporting system for financially motivated cyber crime (a 24/7 reporting service, which forms part of the police)
EU	
Cyber security strategy 7 February 2013	The strategy sets out five priorities: (i) achieving cyber resilience; (ii) drastically reducing cybercrime; (iii) developing cyber defence policy and capabilities related to the Common Security and Defence Policy ("CSDP"); (iv) developing industrial and technological resources for cyber security; and (v) establishing a coherent international cyberspace policy for the European Union and promoting core EU values

Regulation (EC) No 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) 21 May 2013	The Regulation extends the mandate of ENISA for a further seven years. ENISA oversee the promotion of network and information security and are the hub for businesses to share best practices and information on cyber threats with others in their sector across the EU
Cybercrime Directive 12 August 2013, due to be implemented into national law by 4 September 2015	The Directive establishes minimum criminal offences and sanctions for cyber attacks. Companies should make employees aware of the scope of the offences as well as considering their own liability for their employees' actions

UPCOMING LEGISLATION

Name and date of legislation	Aim
UK	
ISO Standard Consultation The results of the consultation were released on 28 November 2013. The new standard is expected to be published in March 2014	The Government decided that as current standards did not fully meet the requirements of participants, they would draw up a new standard, based on the ISO27000-series and focussing on basic cyber hygiene. The aim is that businesses across all sectors will adopt the recommendations in the standard, enabling them to deal with low-level cyber attacks
EU	
Network and information security Directive Proposal going through the EU legislative process with amendments currently being discussed by Parliament. The Commission hopes that the Directive will be adopted by the end of 2014	The current amended proposal of the Directive provides for: (i) national competent authorities and a single point of contact to be set up in each Member State to prevent, handle and respond to network and information security risks and incidents; (ii) a mandatory co-operation mechanism for cyber security information between Member States; (iii) public administrations and private organisations in critical areas (health, energy, transport, finance, internet exchange points and food supply chains) to adopt risk management practices (which can differ depending on the significance of the organisation) and report major security incidents where the disruption is to network information systems related to that organisation's core services and such disruption would have a significant impact in a Member State as a result of the failure of that organisation to maintain its functions; and (iv) Member States to encourage the use of certain European and international interoperable standards and specifications relevant to network and information security, to be determined by a European standardisation body (***see the UK ISO standard consultation above***)

Below is a glossary of some of the more common methods of attack.

See European CSIRT Network Project taxonomy and GovCertUK Incident Response Guidelines for more information.

Name	What it does
General	
Botnets (or zombie armies)	A network of infected computers, which are individually known as zombies (or bots), that can be remotely controlled to perform automated tasks over the internet. Hackers use botnets to launch synchronized attacks, such as DDOS, spam or phishing attacks
Hacking	The unauthorised access to or use of computers and networks, exploiting security vulnerabilities to do so
Availability Attack	
Denial of Service (DOS)	This type of attack aims to flood a server with excessive packets, causing the targeted system to overload and resulting in the failure of particular network services (for example email) or a loss of network functionality, which could lead to a website becoming inaccessible. This attack is normally used to degrade web based services (either static, dynamic or transactional) with the intention of causing reputational damage to the organisation or individual or loss of online revenue
Distributed Denial of Service (DDOS)	Instead of one computer and one internet connection, as is used in a DOS attack above, a DDOS attack relies on botnets, which can be located all around the world, to launch the attack
Information Gathering	
Pharming	Software installed in a system redirects people attempting to access a genuine website to a bogus site
Phishing	Numerous generic emails are sent to people, often posing as being from a trusted entity or promising a reward, to elicit the disclosure of that individual's personal information (e.g. financial details, passwords etc.) or to install malware
Scanning	Attacks that send requests to a system to discover weak points. This also includes some kinds of testing processes to gather information about hosts, services and accounts
Spear Phishing	A more targeted approach to phishing, where attackers may gather information about the target company/individual and will use that information to tailor the phishing email (known as social engineering) to specific individuals making it appear more legitimate

Name	What it does
Malicious Code (or Malware)	
Malicious Code (Malware)	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code, e.g. clicking on a link or an attachment
Spyware	Malware that gathers an individual's sensitive or personal information without their knowledge, which can then be passed on to third parties. Examples of spyware include key-logging software and software that captures screenshots of the victim's computer
Trojan Horses	Malware which appears to be legitimate programs, but allows a computer to be accessed illegally, or may perform malicious unseen functions such as data theft. They may appear to be carrying out a routine job while actually undertaking concealed, unauthorised tasks
Viruses	Malware which can cause minor computer dysfunction, or may have more serious effects, such as damaging or deleting items on a computer. The programs self-replicate, and spread within and between computers. They need to attach themselves to an existing program in a computer which acts as a 'carrier'. They cannot infect a computer without a human action, such as running or opening the infected file
Watering Hole	A web site that has been compromised with the intention to serve malicious code to specific and likely unknown IP addresses with the effect of compromising specific targets of interest
Worms	Another type of malware. Also self-replicating, worms can spread on their own, within and between computers, without needing a host or human action. Even at a minimum they can use up bandwidth, and may be used to allow the creation of a zombie for use in a botnet. They can also be used to place trojans on the network
Fraud	
Unauthorised use of Resources	Using resources for unauthorized purposes including profit-making ventures (e.g. the use of email to participate in illegal profit chain letters or pyramid schemes)
Spoofing	Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it

CYBER SECURITY AT SLAUGHTER AND MAY

Through the joint working of its Technology and Corporate Groups, Slaughter and May helps its clients to manage their 'cyber risks' within their corporate governance structures. This includes assisting with proactive planning, implementation of an information risk management regime and reassurance through corporate governance processes. For more information, please contact:

ROB SUMROY
T +44 (0)20 7090 3061
E rob.sumroy@slaughterandmay.com

FRANCES MURPHY
T +44 (0)20 7090 3158
E frances.murphy@slaughterandmay.com

Detail from Early Morning by Trevor Bell

Returning Value – A different approach?

BACKGROUND

It is a longstanding rule of company law that a proposed distribution of cash or assets to a public company's shareholders (i.e. a "return of value") must be financed either:

- out of the company's distributable profits; or
- with the court's prior approval, out of capital.

Until recently, and following settled precedent, in capital reduction cases the courts have required companies to obtain the express consent of all of their creditors, to pay them, or to secure them in full by ring-fencing cash or liquid investments, or by obtaining bank guarantees. This is obviously impractical for any modern company with substantial permanent debt and a large and diverse body of creditors.

Companies have responded by circumventing these outdated requirements. They did this by introducing a new holding company at the head of their group, through a so-called "new holdco scheme of arrangement". The new holding company could then reduce its own capital, and cash could be up-streamed to it by way of loan in order to fund the return to shareholders. The courts have supported this approach. Although court approval would be required both for the scheme of arrangement and for the reduction of capital within the new holding company, concerns about creditor prejudice simply were not engaged, because the new holding company had no creditors (or, at any rate, none who would not consent). And because the scheme of arrangement was a matter between the company and its shareholders, all of whom were treated equally, and whose overwhelming voting support was assured given that they were the main beneficiaries of this arrangement, there was no basis on which the court could refuse to sanction the scheme of arrangement. As for the creditors of the original parent company, they could not prevent its directors from making a loan to the new holding company; unless, perhaps, they could show that the loan threatened its solvency.

However, introducing a new holding company at the head of a listed group is not without difficulty or expense. A prospectus is required and the new holding company must apply for a new listing. Also, a new holding company can sometimes be ruled out by, for example, contractual or regulatory change of control concerns or by tax legislation (which may result, among other things, in the forfeiture of carried forward losses).

The "real likelihood" innovation a new approach

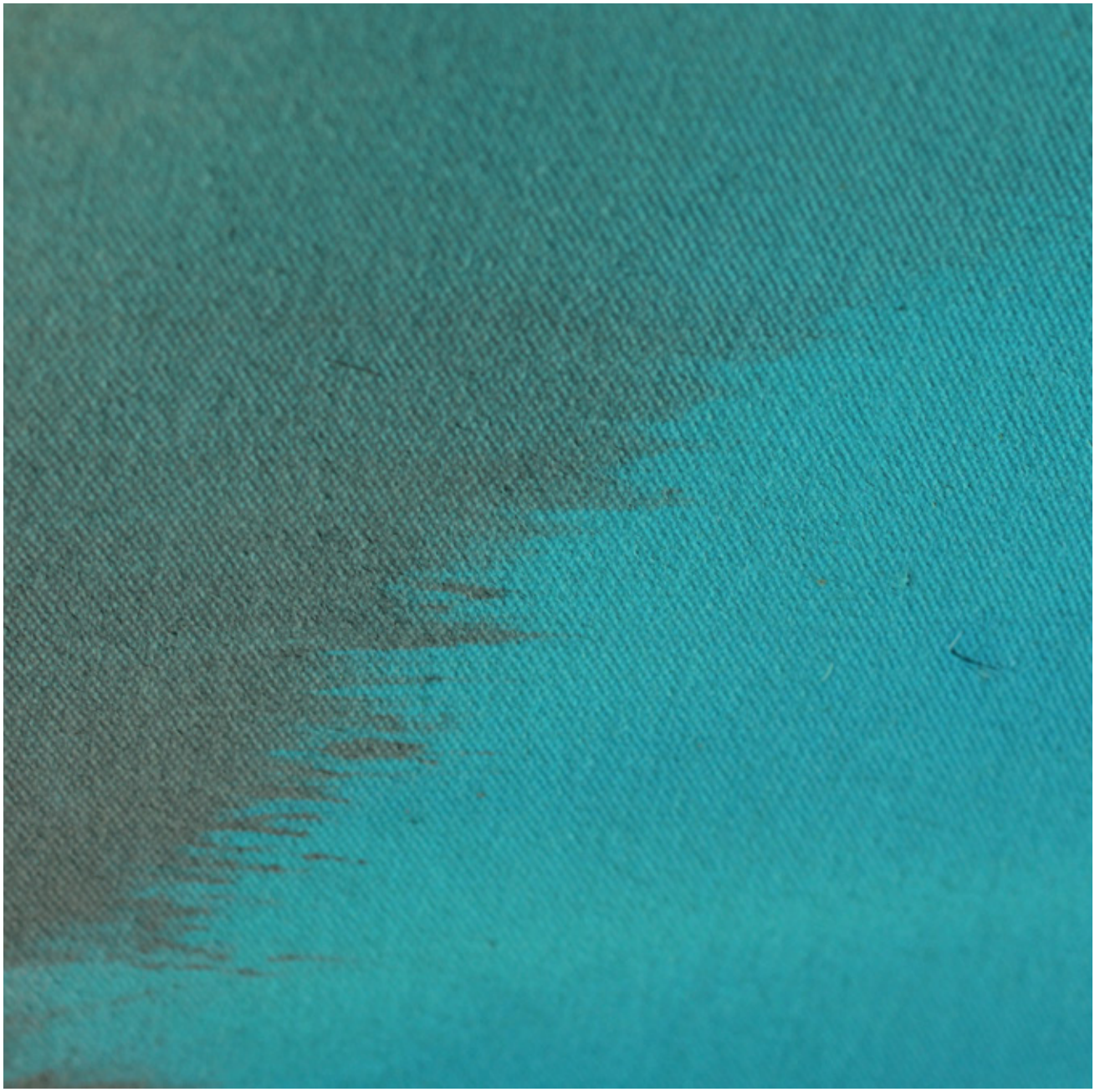
In 2008, changes to the Companies Act 2006 were introduced to provide a more direct route to the summit: if the company could adduce evidence, on an ex parte basis, sufficient to persuade the court that no creditor would be able to show any "real likelihood" of prejudice as a result of the proposed reduction of capital, then the reduction of capital will be confirmed. The new approach was put to the test in the largest ever single return of value by a company anywhere in the world: Vodafone's $84 billion distribution of cash and Verizon shares during February 2014.

To date, the courts have issued guidance on the "real likelihood" test in only three reported cases (the Vodafone judgment will be the fourth). Each of them involved very different circumstances, but none was of comparable scale or complexity, and none of the companies concerned had anywhere near the same diversity in its creditor profile.

The key in a listed company context (and bearing in mind that the proceedings of the court are public) is to provide evidence which satisfies the judge on creditor prejudice issues in the short to medium term while safeguarding potentially sensitive commercial and market information from disclosure. Useful evidence is likely to include a cash flow forecast and expert evidence as to the ability of the company to refinance its debt as it matures (assuming that debt forms a permanent part of its capital structure). Market evidence (for example, credit rating agency reports and pricing data from bond and credit default swap markets) may also be helpful in providing the judge with additional comfort.

CONCLUSIONS

It has long been argued that the capital maintenance rule is inefficient and unnecessary. The advent of the "real likelihood" test, and its successful application in Vodafone's $84 billion return of value, marks a key milestone in the development of company law away from a rigid system of rules towards a more modern, fact-sensitive creditor protection enquiry. While the "new holdco" route is tried and tested, and may remain the preferred option for many, the way is now open for creditworthy companies to return value to shareholders without the cost and complexity of the "new holdco" scheme of arrangement or the need to ring-fence funds to protect non-consenting creditors.



Detail from Sea Morning by Trevor Bell

Miscellaneous Headlines

CORPORATE AND COMMERCIAL

COMPANY AND BUSINESS NAMES REGIME

It was previously reported that, on 4 October 2013, the Department of Business, Innovation & Skills ("**BIS**") published its response to the Government consultation on Company and Business Names (published February 2013) in which the Government proposed to:

- merge the Company and Business Names statutory instruments and Trading Disclosures statutory instruments, so that all requirements can be found in one place;
- reduce the list of "sensitive" words and expressions by approximately one third; and
- reduce the number of words (on the list of those to be disregarded) in the "same as" regulations.

Current indications from BIS are that draft regulations are expected to be published in October 2014.

NEGLIGENT MISREPRESENTATION IN PRE-CONTRACTUAL NEGOTIATIONS

Cramaso LLP v Viscount Reidhaven's Trustees [2014] UKSC 9

The Supreme Court recently considered whether a representation made in the course of pre-contractual negotiations, and responsibility for its accuracy, continued where the identity of the contracting party changed before signing.

In the case in question, the respondents negligently made an implicit misrepresentation in an email to an individual during the course of lease negotiations. The individual subsequently decided to take a lease of the respondents' land, and set up a limited liability partnership ("**LLP**") as the contracting party for the lease, and concluded negotiations as agent for the LLP.

The Supreme Court held that the respondent implicitly repeated the negligent misrepresentation to the individual in his capacity as the LLP's agent until signing, and it continued to be foreseeable that the representation would induce the other party to enter into the contract. As such, the respondents owed the LLP a duty of care, which they failed to fulfil. Accordingly, the respondents were liable to pay damages to the LLP.

LIMITATION OF DAMAGES AND ADEQUATE REMEDY

AB v CD[2014] EWCA Civ 229

The Court of Appeal recently considered the question of damages being an adequate remedy (a factor considered by the courts when exercising their discretion to grant an interim injunction) in circumstances where there the contract contains a limitation on recoverable damages. An appeal was brought by an appellant who had been denied an injunction in these circumstances.

The Court held that the decision of a previous case, *Bath and North East Somerset DC v Mowlem plc [2004] EWCA Civ 115* – where an applicant for an injunction was entitled to argue damages would *not* be an adequate remedy for a threatened breach of contract because the recoverable damages for the expected type of loss were limited under contract – was binding. As such, the appeal was allowed.

The Court's decision was based on the reasoning in *Bath v Mowlem*: (i) the primary obligation of a party is to perform the contract; and (ii) the requirement to pay damages is a secondary obligation, and an agreement to restrict this cannot be treated as an agreement to excuse performance of the primary obligation.

Parties to a contract should, therefore, be aware that limiting the quantum of damages in a contract will not necessarily result in an interim injunction being denied.

ELECTRICITY MARKET REFORM

On 18 December 2013, the Energy Act 2013 received Royal Assent, bringing into law the legal framework for the Government's Electricity Market Reform ("**EMR**") programme. EMR has been designed to incentivise investment in the UK's ageing electricity generating infrastructure and to encourage generators to replace it with a more diverse and low-carbon energy mix.

The first EMR Delivery Plan was published by the Department for Energy and Climate Change on 19 December 2013. The purpose of the EMR Delivery Plan is to set out the Government's long-term energy objectives, key policy decisions to support EMR delivery and supporting analysis.

For more information, please see the *UK Competition and Regulatory Newsletter* (25 Dec 2013 - 07 Jan 2014) available on the Slaughter and May website.

CORPORATE GOVERNANCE

ABI COLLECTIVE ENGAGEMENT

On 12 February 2014, the Association of British Insurers (the "ABI") announced its implementation of recommendations (in its July 2013 report on Improving Corporate Governance and Shareholder Engagement) to establish an Investor Exchange and to invite major shareholders who are not ABI members to join ABI collective engagement meetings. The engagement will be shareholder led, where participants can raise their concerns in relation to a particular UK-listed company, and specify the nature of communication and the identity of those to be approached. So that investor dialogue is not restricted, all Investor Exchange participants will be required to sign a confidentiality agreement, which agreement will permit signatories to share information with other signatories.

FRC REPORT ON IMPLEMENTATION OF THE UK CORPORATE GOVERNANCE CODE

On 19 December 2013, the Financial Reporting Council ("FRC") published its annual report on the impact and implementation of the UK Corporate Governance Code ("CGC") and the Stewardship Codes. The report covers the 12 months since the last FRC report and has three main purposes:

- to report on the quality of reporting against the CGC and Stewardship Codes and on regulatory developments in the UK-listed sector in 2013;
- to give the FRC's assessment on quality of engagement between companies and investors; and
- to indicate where the FRC considers further efforts are required to improve governance and stewardship.

The report noted that, even though most companies were only required to report against the 2012 version of the CGC in 2014, many companies were disclosing their boardroom diversity policies and there had been an increase in the level of audit tendering activity. However, early adoption of the reporting recommendations on the activities of the audit committee and confirmation that the report and accounts are fair, balanced and understandable was less widespread.

In relation to how the CGC had been implemented in 2013, the report focused on: (i) overall compliance rates; (ii) annual elections; (iii) board evaluation; (iv) succession planning and the appointment process; (v) diversity; and (vi) audit tendering.

DISPUTE RESOLUTION

DIRECTORS AND VALIDITY OF SERVICE

Key Homes Bradford Ltd and others v Patel [2014] EWHC B1(Ch)

The High Court recently considered the interpretation of section 1140 of the Companies Act 2006 concerning the service of documents on a director at his "registered address" (being any address shown as a current address in relation to that person in the register available for public inspection).

In the case in question, a claim form was served on the defendant at two addresses in England. The director claimed that this was not valid service under the Civil Procedure Rules ("CPRs") as the addresses were not his usual or last known residential address and he was no longer resident in the UK. The claimant sought to rely on service under section 1140 as the addresses were listed in the register of directors.

The court held that the claim forms *had* been validly served as the section 1140 service provisions (which had been complied with) are separate to, and run parallel to, the service requirements of the CPRs. The court further held that section 1140 is not limited in such a way as to prevent service upon a director who is resident outside of the jurisdiction, so it did not matter that he was not in England at the time.

REFORM OF DEFAMATION LAW

The Defamation Act 2013 came into force on 1 January 2014.

Among other things, the Act removes the presumption in favour of trial by jury in libel or slander claims which will now be tried by a judge alone, unless the court orders otherwise. In addition, a new statutory defence of honest opinion replaces the common law defence of fair comment.

The Act also gives greater protection to operators of websites hosting user-generated content. Under the new provisions, if a defamatory statement is posted on a website, a defence will apply if the operator can show that they did not post the statement on the website, subject to various limitations (including the operator being required to comply with certain procedures in respect of the statement).

NEW ICC MEDIATION RULES

The International Chamber of Commerce ("ICC") launched its new ICC Mediation Rules, which came into force on 1 January 2014. The Mediation Rules replace the ICC ADR Rules that have been used since 2001. The ICC announced that the rules have been adapted to help parties resolve complex cross-border disputes quickly and reliably, and changes include the setting of mediation as the default technique for settling disputes.

LISTING REGIME

ESMA CONSULTATION ON DRAFT REGULATORY TECHNICAL STANDARDS ON MAJOR SHAREHOLDINGS

The revised Transparency Directive (2013/50/EU) was entered into force on 27 November 2013. Among other things, it extended the notification requirements in relation to major shareholdings to financial instruments that have the similar economic effect to holding shares or the right to acquire shares. On 21 March 2014, the European Securities and Markets Authority ("ESMA") launched its consultation on draft regulatory technical standards on major shareholdings, as required under the revised Transparency Directive (see ESMA's consultation paper 2014/300).

The draft regulatory technical standards lay down detailed rules in relation to the implementation of the provisions relating to notification of major holdings under the revised Transparency Directive. They outline: (i) the method of calculating the 5% threshold for the market maker and trading book exemptions to the major holdings notification obligation; (ii) the method for calculating voting rights for certain financial instruments that are referenced to a basket of shares or an index; and (iii) the methods of determining delta for the purposes of calculating voting rights for financial instruments that must be notified on an delta-adjusted basis.

The consultation paper also sets out an indicative list of financial instruments that are subject to the notification requirements under the revised Transparency Directive.

ESMA will consider all comments received by 30 May 2014, and will finalise the draft regulatory technical standards to be submitted to the European Commission by 27 November 2014 for endorsement.

DRAFT COMMISSION DELEGATED REGULATION ON SUPPLEMENTARY PROSPECTUSES

On 7 March 2014, the European Commission published a draft delegated regulation setting out regulatory technical standards for the publication of supplementary prospectuses.

Under the regulatory technical standards, circumstances where a supplementary prospectus must be published include (depending on the type of issuer and prospectus in question):

- where new annual audited financial statements are published;
- where there is an amendment to a profit forecast or profit estimate already included in the prospectus;
- where there is a change of control of the issuer;
- where there is a new public takeover bid by third parties;
- where there is a change in the working capital statement included in a prospectus where the working capital becomes sufficient or insufficient for the issuer's present requirements;
- where an issuer is seeking admission to trading on regulated markets of additional Member States;
- where there is a new significant financial commitment undertaking which is likely to give rise to a significant gross change; and
- where the aggregate nominal amount of the offering programme is increased.

The draft will be passed to the European Parliament and the Council for their consideration.

ESMA'S CONSOLIDATED PROSPECTUS REGISTER

ESMA has compiled an online list of prospectuses and any supplements approved by the national competent authorities of the Member States of the European Economic Area within the last 12 months. Prospectuses can now be searched by retail and wholesale categorisations on the ESMA website.

FCA CONSULTATION ON THE SPONSOR REGIME, THE 28-DAY CIRCULAR AND PROSPECTUS ACCURACY

On 30 January 2014, the Financial Conduct Authority ("**FCA**") announced it is consulting on proposed amendments to the Listing Rules (the "**LRs**") in relation to sponsor competence and other amendments to the LRs and Prospectus Rules (the "**PRs**")(see FCA's consultation paper CP14/2).

Given the importance of the sponsor regime, the FCA stated that they are considering two key aspects: (i) sponsor competency; and (ii) joint sponsor arrangements.

On sponsor competence, the FCA proposed a package of changes to the LRs and Guidance, including: (a) requiring sponsors to have submitted a sponsor declaration to the FCA within the last three years; (b) requiring sponsors to staff sponsor functions with a sufficient number of employees meeting key competencies; and (c) introducing requirements around the "key contact" of a sponsor liaising with the UK Listing Authority ("**UKLA**").

On joint sponsor arrangements, the FCA requested feedback from stakeholders by asking a number of questions to encourage debate on the subject.

The consultation paper also proposed:

- an amendment to the LRs removing the obligation for premium listed companies to prepare a 28-day circular; and
- new PRs placing explicit obligations on those who submit prospectuses to the UKLA for approval to submit a compliant and factually accurate prospectus, to bring the liability regime on prospectuses in line with market practice across other Member States.

The consultation closes on 30 April 2014, and publication of feedback by the FCA is expected in the last quarter of 2014.

CONSULTATION ON CHANGES TO AIM RULES

On 27 January 2014, the London Stock Exchange ("LSE") announced that it is consulting on proposed changes to the AIM Rules for Companies and the AIM Rules for Nominated Advisers (see AIM Notice 38).

Proposed changes to the AIM Rules for Companies are mainly of an administrative and clarificatory nature, including:

- clarifying that the LSE has jurisdiction over AIM companies that cease to be admitted to AIM in relation to breaches or suspected breaches of the AIM Rules at a time when the company did have securities admitted to AIM; and

- amendments to the rule relating to the disclosure of price sensitive information, including replacing the reference to a "substantial" price movement in the AIM security with "significant", to bring the terminology in line with that used in the Financial Services and Markets Act 2000.

The consultation closed on 3 March 2014, and it is currently intended that the new rules will come into effect during 2014.

CHANGES TO THE LISTING RULES RESULTING FROM DIRECTORS' REMUNERATION REGIME

On 13 December 2013, the FCA published policy statement PS13/11, which made changes to the LRs resulting from the Directors' Remuneration Reporting Regulations [SI 2013/1981] and Narrative Reporting Regulations [SI 2013/1970]. The changes to the LRs were made to reduce the overlap between the LRs requirements and the new Directors' Remuneration Reporting Regulations.

The new LRs came into force on 13 December 2013 for listed companies with a financial year ending on or after 30 September 2013 that had not published their annual report on or before 13 December 2013. This came into force earlier than initially expected. Companies already preparing their annual report in compliance with both the old LRs and the new Directors' Remuneration Reporting Regulations can publish that report after 13 December 2013 in accordance with both sets of requirements, if they choose to do so.

OPINION ON PUBLICATION OF PROSPECTUSES IN ELECTRONIC FORM

Michael Timmel v Aviso Zeta AG (Case C-359/12)

On 26 November 2013, Advocate General Sharpston delivered her opinion on *Timmel v Aviso Zeta*, a case before the Court of Justice of the European Union ("CJEU") that concerns how issuers should publish their prospectuses. The opinion argues that a prospectus that is hyperlinked electronically to a website will not be validly published if access to the prospectus is subject to certain conditions such as acceptance of a disclaimer.

The prospectus in question was available electronically on the homepage of the Luxembourg Stock Exchange. To access the prospectus via the website, it was necessary to register a user's account, provide an email address and accept a disclaimer. Even after registration, it was only possible to access two documents a month without paying a fee.

A question was referred to the Advocate General (among other questions) whether the requirement laid down in Article 29(1)(1) of the Prospectus Regulation (Regulation No 809/2004 of the European Commission) – that the prospectus or the base prospectus must be "easily accessible when entering the web-site" – would be fulfilled if access is subject to certain conditions.

The Advocate General concluded that it is incompatible with Article 29 to make access via a website to a prospectus or to a base prospectus subject to conditions such as: (i) requiring registration that involves acceptance of a disclaimer and provision of an email address; or (ii) requiring payment; or (iii) restricting free access to the required information under the Prospectus Regulation to two documents per month. Issuers may find it interesting

to note that the Advocate General acknowledged that we are now in "the information age", but stated that it did not follow that all potential investors have an email address and, as such, any condition requiring provision of an email address would automatically exclude any investor who does not use email.

FINANCIAL REGULATIONS

BANKING REFORM BILL RECEIVES ROYAL ASSENT

The Banking Reform Bill received Royal Assent on 18 December 2013 as the Financial Services (Banking Reform) Act 2013.

The Act contains provisions to implement the recommendations of the Independent Commission on Banking that was set up to consider structural reform of the banking sector, including those in relation to the retail bank ring-fencing framework. It also implements the recommendations of the Parliamentary Commission on Banking Standards, which was asked by the Government to review professional standards and culture in the banking industry.

Among other things, the Act:

- introduces a bail-in regime;
- establishes a new Payment Systems Regulator;
- replaces the approved persons regime with a senior persons regime; and
- provides for a new criminal offence of reckless misconduct in the management of a bank.

FINANCIAL REPORTING

NEW EUROPEAN TRANSPARENCY RULES ON SOCIAL RESPONSIBILITY FOR BIG COMPANIES

On 26 February 2014, the Committee of Permanent Representatives ("COREPER") endorsed the agreement reached between the Council of the European Union and the European Parliament on a draft directive for the disclosure of non-financial and diversity information by certain large companies. New measures, which are yet to be formalised, will require certain big EU companies to draw up a statement relating to environmental, social and employee-related matters, respect for human rights, anti-corruption and bribery matters on an annual basis. The statement will have to include a description of the policies, outcomes and the risks related to those matters.

It is expected that the European Parliament will vote this legislation in plenary in April 2014, and the Council will formally adopt it subsequently.

EUROPEAN REFORMS TO THE AUDIT MARKET

On 18 December 2013, COREPER endorsed the agreement reached between the Council of the European Union and the European Parliament on the reform of the audit market in the EU. This follows the European Commission's legislative proposal to amend the Statutory Audit Directive and introduce a new regulation regarding the statutory audit of public-interest entities ("PIEs").

The new legislation will:

- impose mandatory rotation of auditors of PIEs after 10 years; and
- prohibit a number of non-audit services, such as tax, consultancy and advisory services, to be provided to the audited entity to avoid conflicts of interests and threats to independence.

The agreement still remains subject to formal approval.

FRC AUDIT QUALITY THEMATIC REVIEW ON MATERIALITY IN AUDIT

On 16 December 2013, the FRC published a report on a thematic inspection review undertaken by its Audit Quality Review team during 2013. The theme for the review was the auditor's consideration and application of materiality.

The FRC states that the finding and recommendations should assist auditors in reviewing current guidance and practices at their firms and Audit Committees in discharging their oversight responsibilities.

The FRC notes that Audit Committees play an essential role in ensuring the quality of financial reporting, particularly their work in discussing with auditors the audit plan and the audit findings. As such, the FRC made a number of recommendations that they believe may enhance their oversight of the audit process in relation to materiality, thereby contributing to an overall improvement in audit quality. These include Audit Committees seeking to understand: (i) the basis for materiality levels set, including how they reflect the needs and expectations of users of the financial statements; (ii) how materiality levels might affect the level of audit work performed; (iii) the benchmarks used by the auditors in determining materiality levels; (iv) the reasons for, and the effect of, any increases in materiality levels; (v) why management have not adjusted the financial statements for uncorrected misstatements brought to their attention by the auditors; and (vi) whether disclosure omissions reported to them have arisen through error or a specific management judgement.

FRC WARNS AGAINST CLASSIFYING PENSION LIABILITIES AS EQUITY

On 15 January 2014, the FRC issued a press release warning boards against entering into arrangements that turn pension obligations into equity instruments in their accounts.

The FRC has warned companies and their advisers that its Financial Reporting Review Panel will ordinarily open an enquiry into the financial reporting of any company in which material pension liabilities are reclassified from debt to equity.

PRIVATE EQUITY

2014 GUIDE FOR GOOD PRACTICE REPORTING BY PRIVATE EQUITY PORTFOLIO COMPANIES

On 5 February 2014, the Guidelines Monitoring Group ("GMG") published an updated version of its guide on good practice reporting by private equity portfolio companies. The guide is intended to assist private equity owned portfolio companies in improving transparency and disclosure by highlighting good practice examples. The guide is also intended to help portfolio companies conform under the Walker Guidelines and to understand the appropriate level of disclosure.

TAKEOVERS

TAKEOVER PANEL STATEMENT ON CONCERT PARTIES

On 5 March the Takeover Panel published Panel Statement 2014/3 regarding concert party and Rule 9 (mandatory offer) issues relating to an assignment of a loan and the subsequent enforcement of a related charge over shares. The Policy Statement provides an example of the Panel's application of the dispensation from Rule 9 where a lender would otherwise incur an obligation to make a mandatory offer under Rule 9, and the related requirement to dispose of shares and restrict voting rights in those circumstances.

London
One Bunhill Row
London EC1Y 8YY
United Kingdom

T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Brussels
Square de Meeûs 40
1000 Brussels
Belgium

T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
47th Floor, Jardine House
One Connaught Place
Central
Hong Kong
T +852 2521 0551
F +852 2845 2125

Beijing
2903/2905 China World Office 2
No.1 Jianguomenwai Avenue
Beijing 100004
People's Republic of China
T +86 10 5965 0600
F +86 10 5965 0650