Ashurst London
June 2013

Corporate briefing

Cyber attacks: a briefing for boards

Introduction

Recent years have seen a number of high profile cyber attacks and data security breaches that have affected a wide range of businesses, including some of the world's best known technology companies. An "information security breaches" survey published in April, commissioned by the Department for Business Innovation & Skills (BIS) and conducted by PwC, has shown that the number of security breaches affecting UK businesses continues to increase. According to the survey, 93 per cent of large businesses and 87 per cent of small businesses have had a cyber security breach in the last year.

The Institute of Chartered Secretaries and Administrators, together with BIS, last week published a guidance note on cyber risks aimed at boards of listed plcs, outlining issues for boards and risk management strategies (ICSA Guidance).

In this briefing we examine, from a legal perspective, how to prepare for the eventuality of a cyber attack and what to do after the event if you are attacked.

What is cyber crime?

Cyber crime is an umbrella term that includes a number of different types of attack, for example, distributed denial of service attacks (DDOS), botnets, phishing scams, spamming and virus and malware infections. All have the effect of compromising the integrity, confidentiality or performance of a company's computer system and the data stored within that system. They are carried out for a number of different reasons, including the desire to: steal information, obtain publicity and/or damage or overload a business's computer systems, either in retaliation for something that business has done or because the attacking party perceives that business to be a threat. The victim of a cyber crime can suffer a wide variety of loss, including damage to reputation, loss of revenues, litigation costs and the costs of repairing computer systems or restoring damaged data.

The role of the board

The ICSA Guidance emphasises the key role that boards of listed plcs should play in assessing the risk of cyber attacks. Boards should provide ultimate oversight of the risk, with the assistance of the audit committee, perhaps appointing one director to have specific responsibility for this area. When undertaking the risk assessment, the board and audit committee should focus on the consequences of a cyber attack. The ICSA Guidance also sets out a list of key questions for the board to ask management. Once the risk is assessed and control procedures are put in place, the board should monitor the procedures to assess their effectiveness. These should include the appointment of key individuals who can respond quickly to minimise the consequences of any cyber attack. The board should also challenge those responsible for cyber risk to satisfy itself that a thorough assessment has been carried out and that risk management procedures are robust. Because of the relative novelty and uniqueness of the risks arising in this area, boards will have to consider whether their existing procedures are sufficient to cope with cyber risk.

Benefits of a robust cyber crime strategy

Once the risks to be protected against have been assessed, there are a number of practical steps that a UK business can take to form a robust cyber security strategy. The first step is to decide what assets the company needs to protect, whether they are: employee or customer personal data, intellectual property and confidential information or the continuity and reliability of its computer systems. Next a company must decide the level of risk which it is willing to accept. No defence strategy will provide a guarantee that no attack will get through and so ultimately it comes down to a cost-benefit analysis. In order to understand the cost-benefit ratio of implementing a robust cyber security strategy, a company must understand not only the value of the assets it wishes to protect but the regulatory and legal obligations with which it must comply.

In order to halt an erosion of public trust and to mitigate against the economic damage caused by cyber crime, a number of steps have recently been taken by law makers. These include a new cyber security Directive proposed by the EU Commission and a move by BIS to select and endorse an organisational standard for cyber risk management (see paragraph headed "The future" below).

Until the new Directive is implemented, the UK regulatory requirements that apply to cyber security have been enacted to respond to other policy concerns. For example, the Data Protection Act 1998 requires those who process personal data to have in place appropriate technical and organisational measures against unauthorised or unlawful processing of personal data. There are also a number of sector-specific regulatory obligations which relate only to FCA regulated firms. Where businesses operate outside the UK, they should investigate the regulatory regimes in those jurisdictions and take account of EU/UK data protection law which places restrictions on the export of data outside the European Economic Area.

Contractual considerations

The damage that can be caused by a cyber attack is much wider than simply damage to computer systems or data and associated regulatory breaches. If, as is commonly the case, a company's computer systems form an integral part of the company's business then an attack can cause a company to fail to meet its contractual obligations. Unless a company can meet the stringent test of contractual frustration, i.e. that the attack caused a material change in circumstances which rendered the contract impossible to perform or deprived it of its material purpose, a company must rely on explicit contractual provisions to remove or put on hold its obligations. The most likely candidate is a force majeure clause, which may negate an attacked party's contractual obligations if sufficiently broad language has been drafted. It is worth noting that force majeure clauses that list the type of events that will cause the clause to activate (e.g. "terrorism", "act of God", etc.) often make no reference to cyber attacks. A full audit of key contractual arrangements is an important step that a business should take when putting in place its cyber security strategy. Going forwards, you may want all new contracts to be drafted with cyber security in mind, whether implicitly or explicitly.

Implementing the strategy

Once a robust cyber security strategy has been devised there are a number of additional steps that a business can take to ensure that the strategy is implemented effectively. Since any cyber security defence is only as strong as its weakest link, businesses should invest in staff training to ensure that the strategy is understood and implemented uniformly. An effective tool is to draft an internal user security management policy which sets out what training will be carried out, instructions in the use of computer systems and passwords, and the reporting processes that should be followed in the event of an attack. A business may want to supplement its security management policy with a home and mobile working policy governing the use of computer systems remotely, especially with regard to employees that have been permitted to connect to the company's systems with their own devices. A company should also have in place a business continuity plan that sets out how the business will operate in the event of a cyber attack which, for example, shuts down its IT systems or those of its key service providers. Businesses which have outsourced key business processes will want to ensure that their outsourced service providers have back up systems and a disaster recovery and business continuity plan in place to respond adequately to cyber attack. As part of any tendering process, the business should assess the ability of its service provider to withstand cyber attacks.

Once a cyber security strategy has been put in place, a business can consider how else it can bolster its cyber security protection, for example, through insurance. Since cyber crime is still not a typically-insured risk, businesses should check with their insurer as to whether or not they are covered. In considering whether to take out additional cyber crime liability insurance, a business should weigh the policy premiums against the risk and expense of suffering an attack. As cyber crime insurance is still a nascent market, negotiating a bespoke policy may be the best way a business can ensure it is covered for a reasonable premium. The terms of the policy should be checked to ensure that the cover is suitable, for example, the policy is unlikely to cover regulatory fines or losses incurred by third parties.

Reporting an attack

If a business should fall victim to a cyber attack, it should immediately consider what reporting obligations, if any, the business has.

Listed companies should consider whether the attack should be reported as inside information to the market pursuant to the Financial Conduct Authority's Disclosure and Transparency Rule (DTR) 2.2.1R. This will obviously depend on the severity of the attack and the nature of the company. It may be possible to

delay a detailed announcement if further time is needed to judge the severity of the attack and the consequences (DTR 2.2.9G), although in this situation a holding announcement may be required. Depending on the nature of the attack, the company may consider that it can no longer comply with Listing Principle 2 (which requires it to take reasonable steps to establish and maintain procedures, systems and controls to comply with its obligations as a listed company) because a breakdown in its internal reporting lines might mean that it cannot comply with the basic requirement in DTR 2.2.1R to announce inside information to the market. The company could also be in breach of Listing Principle 4 (the requirement to communicate information to shareholders in such a way as to avoid the creation of a false market). In these situations, the company should seek advice from a sponsor who in turn should speak to the Financial Conduct Authority as necessary.

Data protection

With regard to data protection, the Information Commissioner's Office (ICO) takes the view that controllers of personal data should report to it serious breaches of security which result in the loss, release or corruption of personal data. Although this is not yet a legal obligation it is likely to be considered a mitigating factor in the event the company is subject to sanctions (e.g. a fine) and may act to limit some of the reputational damage that is caused in the event that the breach becomes public.

ENRC: recent case study

A recent example of a listed company reporting a cyber attack to the market is Eurasian Natural Resources Corporation PLC, which on 23 May announced two breaches relating to (1) theft of a laptop computer and (2) an attack on its computer systems by a third party. Both of the breaches were reported to the ICO. The announcement also noted that affected staff had been provided with guidelines on precautionary actions and that the company and its group had reviewed and upgraded its systems to prevent such incidents taking place in the future.

The future

On 2 February 2013 the EU Commission published its cyber security plan designed to protect internet freedom and opportunity, which included a proposal for a new cyber crime Directive to ensure a high standard of information security across the EU. Under the proposal, any company which operates critical infrastructure will be obliged to report a cyber attack. "Critical infrastructure" is defined widely and includes not just energy companies, banks and hospitals but companies which provide e-commerce platforms, cloud computing services, search engines, internet payment gateways and even social networks. On a national level, EU Member States will also be required to create a national competent authority, the Computer Emergency Readiness Team (CERT), to handle incidents and risks, and will be required to share information on cyber crime with other Member States.

The proposed new data protection regulation announced on 25 January 2012 by the EU Commission contains a range of measures, some of which relate to cyber security. In particular, the proposed regulation introduces an obligation to notify supervisory authorities and data subjects of data breaches without undue delay (or within 24 hours, where possible, in the case of notification to supervisory authorities) (see our January 2012 Data Protection Briefing "Proposed reforms to EU data protection law").

The are also national measures to bolster UK businesses' cyber security credentials. Following the guidance published by BIS in September 2012, on how to guard against cyber crime threats and in which areas security should be improved, the Government has launched a consultation on cyber security organisational standards. It plans to select and endorse an organisational standard which businesses can implement to ensure effective cyber security risk management. The consultation closes on 15 October 2013.

How we can help

We can provide assistance in relation to setting up your cyber security strategy and in the event you suffer a breach. For example we can:

- work with you and your IT consultants to produce a cyber security policy;
- provide information on the current regulatory environment;
- assess your contracts for cyber security compliance;
- provide advice on any legal implications and notification requirements in the event of an attack;
- defend you against third party claims; and
- explain the changing regulatory landscape and how it will affect your business.

Key contacts

Please contact one of the authors below or one of the Ashurst corporate partners listed if you wish to discuss any of the points raised in this briefing.

Mark Lubbock
Partner, London

T: +44 (0)20 7859 1762
E: mark.lubbock@ashurst.com

Matthew Noble
Solicitor, London

T: +44 (0)20 7859 3227
E: matthew.noble@ashurst.com

Corporate Partners			
Rob Aird	London	T: +44 (0)20 7859 1726	E: rob.aird@ashurst.com
Hammad Akhtar	London	T: +44 (0)20 7859 1720	E: hammad.akhtar@ashurst.com
Simon Baskerville	London	T: +44 (0)20 7859 1141	E: simon.baskerville@ashurst.com
Chris Bates	London	T: +44 (0)20 7859 2388	E: chris.bates@ashurst.com
Simon Beddow	London	T: +44 (0)20 7859 1937	E: simon.beddow@ashurst.com
Jeremy Bell	London	T: +44 (0)20 7859 1913	E: jeremy.bell@ashurst.com
Giles Boothman	London	T: +44 (0)20 7859 1707	E: giles.boothman@ashurst.com
Nick Bryans	London	T: +44 (0)20 7859 1504	E: nick.bryans@ashurst.com
David Carter	London	T: +44 (0)20 7859 1012	E: david.carter@ashurst.com
Nick Cheshire	London	T: +44 (0)20 7859 1811	E: nick.cheshire@ashurst.com
Anthony Clare	London	T: +44 (0)20 7859 1927	E: anthony.clare@ashurst.com
Adrian Clark	London	T: +44 (0)20 7859 1767	E: adrian.clark@ashurst.com
Karen Davies	London	T: +44 (0)20 7859 3667	E: karen.davies@ashurst.com
Karan Dinamani	London	T: +44 (0)20 7859 1130	E: karan.dinamani@ashurst.com
Jonathan Earle	London	T: +44 (0)20 7859 1126	E: jonathan.earle@ashurst.com
Ray Fisher (US)	London	T: +44 (0)20 7859 1797	E: ray.fisher@ashurst.com
Charlie Geffen	London	T: +44 (0)20 7859 1718	E: charlie.geffen@ashurst.com
Nick Goddard	London	T: +44 (0)20 7859 1358	E: nick.goddard@ashurst.com
Richard Gubbins	London	T: +44 (0)20 7859 1252	E: richard.gubbins@ashurst.com
Bruce Hanton	London	T: +44 (0)20 7859 1738	E: bruce.hanton@ashurst.com
Nicholas Holmes	London	T: +44 (0)20 7859 2058	E: nicholas.holmes@ashurst.com
Isabelle Lentz	London	T: +44 (0)20 7859 1094	E: isabelle.lentz@ashurst.com
Adam Levitt	London	T: +44 (0)20 7859 1633	E: adam.levitt@ashurst.com
Stephen Lloyd	London	T: +44 (0)20 7859 1313	E: stephen.lloyd@ashurst.com
Mark Lubbock	London	T: +44 (0)20 7859 1762	E: mark.lubbock@ashurst.com
Tom Mercer	London	T: +44 (0)20 7638 1111	E: tom.mercer@ashurst.com
Rob Moulton	London	T: +44 (0)20 7859 1029	E: rob.moulton@ashurst.com
Sergei Ostrovsky	London	T: +44 (0)20 7859 1821	E: sergei.ostrovsky@ashurst.com
David Page	London	T: +44 (0)20 7859 1908	E: david.page@ashurst.com
Jonathan Parry	London	T: +44 (0)20 7859 1086	E: jonathan.parry@ashurst.com
James Perry	London	T: +44 (0)20 7859 1214	E: james.perry@ashurst.com
Michael Robins	London	T: +44 (0)20 7859 1473	E: michael.robins@ashurst.com
Eavan Saunders Cole	London	T: +44 (0)20 7859 1838	E: eavan.saunderscole@ashurst.com
Jennifer Schneck (US)	London	T: +44 (0)20 7859 1744	E: jennifer.schneck@ashurst.com
Mark Sperotto	London	T: +44 (0)20 7859 1950	E: mark.sperotto@ashurst.com
Nigel Stacey	London	T: +44 (0)20 7859 1028	E: nigel.stacey@ashurst.com
Jeffrey Sultoon	London	T: +44 (0)20 7859 1717	E: jeffrey.sultoon@ashurst.com
Piers Warburton	London	T: +44 (0)20 7859 1099	E: piers.warburton@ashurst.com
Nick Williamson	London	T: +44 (0)20 7859 1894	E: nick.williamson@ashurst.com