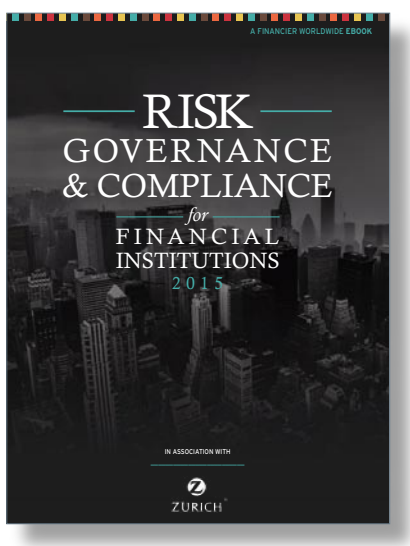
REPRINT

FINANCIER WORLDWIDE corporatefinanceintelligence

CYBER-ATTACKS – THE GLOBAL RESPONSE

REPRINTED FROM:
Risk, Governance & Compliance for Financial Institutions 2015



www.financierworldwide.com

Visit the website to request a free copy of the full e-book

GIBSON DUNN

Published by Financier Worldwide Ltd

CYBER-ATTACKS – THE GLOBAL RESPONSE

BY SELINA SAGAYAM, ALEX SOUTHWELL AND DAVID DOWLING
GIBSON DUNN & CRUTCHER LLP

Cyber security and hacking have steadily risen up the popular, economic and political agenda, culminating in a flurry of activity at the start of 2015. In September 2014, it was revealed that hackers had accessed the accounts of dozens of celebrities. This Hollywood leak was soon followed by another in November 2014, targeted against Sony Pictures and seemingly in response to the proposed release of 'The Interview'. However, it was not only the entertainment industry that suffered attacks. During January 2015, the Twitter and YouTube accounts of the US Central Command were hacked by groups claiming to support Islamic State. Nor is it only traditional companies that have suffered from cyber attacks. In February 2014, hackers led to the temporary closure of the two primary trading exchanges for bitcoin, the electronic currency. Customers were left unable to withdraw their funds, while the attacks continued. In 2014, the UK government's intranet had been attacked by a

'state sponsored battle group'.

What is patently clear from the recent spate of attacks is that all sectors of society – businesses, governments, community and social – face the real threat of a cyber attack. This realisation and other events have pushed cyber security concerns to the top of the agenda around the globe, with President Obama using his State of the Union Address in January 2015 to propose new measures to combat cyber attacks. A few days later at the annual meeting of the World Economic Forum in Davos, there were many calls for increased resources and cooperation to tackle the issue.

This article takes a look at recent legislative and operational developments in the US, UK and EU in response to this ever growing threat.

UNITED STATES

Among other proposals, President Obama has proposed three bills in the US in a three-pronged approach to combat cyber attacks. The legislation covers information sharing, prosecutions and data protection issues. In particular, the legislation: (i) aims to increase information sharing between the public and private sector, as well as collaboration within the private sector; (ii) increases the powers of federal law agencies to prosecute the sale of botnets and stolen financial information; and (iii) proposes a national procedure relating to data breach notifications.

EUROPE

By the end of January 2015, the EU was in the final stages of considering the proposed cyber security Network and Information Security Directive, colloquially known as the Cyber Directive. The main outstanding issue for EU legislators is the scope of the directive – in particular, whether or not

certain operators in identified sectors and internet operators would be subject to the obligations regarding security requirements and incident notifications in the Directive. The Directive will create a duty of care on organisations to maintain a high level of cyber security and requires certain industries to adopt tough security measures and serious breaches of security to their respective national regulators.

The Directive also creates a new EU-wide regulatory framework to be run by a new pan-European agency (ENISA) which will issue guidance and enforcement. EU member states will be required to publish a cyber security strategy and create a computer emergency response team to monitor cyber issues. Each member state will need to designate its own 'cyber regulator' to oversee and operate the sanctions regime.

THE UK RESPONSE

Cyber security has been an increasing focus of the UK Government's agenda too. In November 2011, the UK Cabinet Office launched National Cyber Security Programme outlining steps that the government would take to tackle cyber crime by 2015.

No new legislation has been promulgated but a number of other initiatives have been undertaken as a result of the strategy. In December 2013, a set of Guiding Principles on Cyber Security, developed between the Department for Business, Innovation and Skills (BIS) in the UK and leading ISPs, was published. In January 2014, the UK government in partnership with the Institute for Chartered Accountants in England and Wales and working with other leading UK industry organisations, produced a guide on cyber security in the context of corporate finance transactions. More recently, in January 2015, BIS published updated guidance for businesses on how to recognise and prepare for cyber attacks. The UK government has also helped businesses by launching the 'Cyber Essentials' scheme which

sets out 10 guiding principles on how to mitigate risk from basis internet based threats and provides an assurance scheme so that businesses can demonstrate to their customers, suppliers and other third parties that they have taken these essential precautions. On a more industry specific level, CBEST, the Bank of England's cyber crime framework, was established in June 2013 to coordinate the Bank's response to cyber threats to firms deemed 'core' to the UK financial system with input from government security agencies.

How has the UK fared? Has the strategy to combat cyber attacks by 2015 been successful? Data from 2014 is not particularly encouraging. A study of APT (Advanced Persistent Attacks) in EMEA revealed that Britain suffered significantly more attacks than any other state in Europe or the Middle East. A recent report produced by GCHQ (the UK's electronic surveillance agency) stated that more than 80 percent of the UK's largest companies suffered an attack in 2014, costing each company between £600,000 and £1.5m. What more needs to be done?

AN APPROPRIATE RESPONSE – INTERNATIONAL COOPERATION

International cooperation is essential in the war against cyber attacks, particularly given the cross-border nature of many cyber attacks and the exchange of information across borders. There has been more recently an increased focus on the importance of collaboratively dealing with cyber security. In an example of recent transatlantic cooperation, UK prime minister Cameron and president Obama announced that the US and UK would carry out joint simulation cyber attacks. Targets of these electronic war games will include the Bank of England, commercial banks in the City of London and Wall Street, as well as critical energy and transport infrastructure.

AN APPROPRIATE RESPONSE: PRE-EMPTIVE ACTION

Cyber security was a key topic at the World Economic Forum this year. The backdrop was ominously laid out as Cisco's CEO warned that 2015 will be even a worse year for cyber attacks than 2014. Several banks at Davos expressed a desire to be able pursue an 'active defence' in locating and destroying hackers' servers. Industry experts suggest that this tactic is currently more commonly considered in the US than in Europe. Indeed, in the UK, the Computer Misuse Act makes it illegal for a bank to carry out any cyber strike against another computer in the country.

Despite some companies preparing aggressively to respond to cyber attacks, a recent survey found that fewer than 40 percent of boards regularly receive reports on privacy and security and 26 percent rarely or never receive such information. In today's environment, boards must seek to educate themselves on cyber security issues. However, both internal technical experts and external consultants must ensure that the board understands that cyber security is a commercial risk, not just an IT concern. In addition, boards need to be given up-to-date information to be able to understand what steps are being taken and whether these are sufficient. Several companies have already or are currently in the process of updating the responsibilities of the board's audit committee to specifically reference reviewing the company's cyber security programs.

AN APPROPRIATE RESPONSE: BEST PRACTICE ON M&A DEALS

Given the potentially devastating financial and operational costs of a cyber attack, dealmakers ought to be alive to cyber security issues. For potential purchasers, it is not a question only of undertaking appropriate due diligence or ensuring adequate, tailored contractual protection to

address cyber risks and threats. In their guide to cyber security, the ICAEW draw attention to several instances of a purchaser company being infected by hackers as a result of integrating a new subsidiary with poor cyber security protections – this is identified as a critical time of vulnerability for businesses. Another vulnerable time on transactions is when consideration monies are being transferred.

However, even before a deal is made, cyber risks are plentiful. For example, virtual data rooms represent an opportunity for hackers to access sensitive information about the company and its customers/ employees. There are also regulatory implications if inside information is inadvertently leaked or exploited during the deal process, a period when increased numbers of people have access to data.

AN APPROPRIATE RESPONSE: INSURANCE?

In addition to the growth in cyber security firms, insurance companies are also paying particular attention to the increased focus on the risks of cyber attacks offering a range of cyber risk policies.

Many US states require companies to inform their customers in the event that their data has been compromised. As well as the costs associated with such a notification, companies are seeking to insure themselves against conducting an investigation, crisis and reputation management and, most significantly, lost business. Loss of business is a key concern for companies, with a recent PwC report showing that 61 percent of customers would move their business away from a company that has had data compromised by a cyber incident.

WHO IS BENEFITING?

Everything is not doom and gloom however. Not everything about the rise of cyber attacks is bad for investors, particularly those interested

in investing in the 'guardians of the internet'. Business is booming for the cyber security industry, with venture capital funding for the sector rising by a third to $2.3bn during 2014, according to PrivCo, a research company. One beneficiary of this surge is Ionic Security, which raised $40m in its recent funding round, twice as much as it did the previous year. Internet security firm FireEye Inc., which made its market debut in September 2013 at US$20 per share, is now trading at $36.02, valuing the company at over $5.4bn.

Another example of this growth is the Virtual Technology Centre (VTC) in Hampshire, England, a project specifically praised by David Cameron. In January 2015, Lockheed Martin UK, a subsidiary of the US defence and security company, announced that it had entered into a partnership with Restoration Partners, the boutique technology merchant bank, to create the VTC. The VTC is designed to encourage SMEs working in cyber security by providing them with a hub of expertise, and follows existing investment of more than £40m in facilities in Hampshire, including a £30m innovation laboratory.

CONCLUSION

The cyber security landscape is changing fast, and companies need to make sure that they are adequately protected. On both sides of the Atlantic, new legislation is expected to come into force, and companies should seek proper advice to ensure they are compliant.

Selina Sagayam is an international corporate finance partner, Alex Southwell is co-chair of the Information Technology and Data Privacy Practice Group and David Dowling is an associate at Gibson Dunn & Crutcher LLP.