A BIBA broker's guide to...

Cyber risks

2014 - Issue 3

Part 2: Business Interruption

BIBA

In association with DAC beachcroft ZURICH

Foreword

STEVE WHITE
CHIEF EXECUTIVE
BIBA

Cyber security issues continue to fill the headlines on a national and international scale. Names like "heartbleed", "GoZeuS", and "Cryptolocker" might sound like something out of a Hollywood blockbuster but they are, unfortunately, today's reality of conducting business in an electronic world.

The Government has long since recognised cyber threats, not only to UK security interests, but the effects on GDP via business and industry. As long ago as 2011, at a time of significant public spending cuts, the UK Government announced an investment of £650m in cyber security. This investment is now bearing fruit including recently launched schemes and partnerships that will help organisations to improve their cyber resilience.

BIBA is pleased to be playing its part by working with the Government on such initiatives, including the Cyber Essentials Scheme which was announced in June 2014. The Government will lead the scheme by requiring any of its high-risk suppliers to be certified but there are compelling reasons for any company to seek accreditation.

The scheme is one of a number of recent developments in the cyber risk space which can help businesses improve their own cyber security. We all have a duty to improve the UK's cyber resilience and in this guide we highlight some of the most recent resources that organisations can draw upon so that we can play our part.

This series of legal supplements is brought to you through a partnership of BIBA, DAC Beachcroft and Zurich. We hope that you find DAC Beachcroft's legal expertise, Zurich's industry knowledge and BIBA's desire to share these with you helpful and we welcome any suggestions for future subjects.

Introduction

This is the second of two publications on cyber risks. In this publication, we focus on business interruption, or disruption, that can be caused by cyber incidents. The case study set out on the following pages explains the risks faced by businesses' reliance on electronic systemsin the modern age.

When considering how a business might be affected by cyber risks, it is important not to overlook functions that might not immediately appear as business critical. The ability for support functions to operate can be just as important as front of house operations. For example, a company that considered their online presence as a low risk because they only used their website to process service enquiries rather than sales, realised they could suffer contractual penalties and reputational harm when their website was hacked and they could no longer process those service enquiries.

This guide looks at a number of existing and recently launched resources which can help organisations assess and reduce their exposures at both a technical and organisational level. This guide merely scratches the surface on the wealth of available guidance and we recommend that companies seek professional advice if they have concerns in this area.

Exposure to business interruption caused by cyber risks has grown for a number of reasons including:

- an increasing reliance on electronic systems to conduct business;
- the automation of business functions which are reliant on electronic systems; and
- the interconnectivity of those electronic systems, to internal and external networks.

Hans Allnutt
Partner
DAC Beachcroft LLP

Patrick Hill
Partner
DAC Beachcroft LLP

Case Study:

LOCKYERS INSURANCE

My name is Jon Newall and I'm Principal of Lockyer Insurance. We are an independent broker, based in Wakefield, West Yorkshire. We handle business locally and across the UK and have grown significantly in the past few years.

We specialise in commercial insurance and provide cover for a wide range of SMEs through to complex risks such as mines and piers. We have strong relationships with a wide range of insurers and are also members of the Broker Network, which gives us powerful buying power, without compromising our independence.

Our core strength is the high level of personal service we provide - from risk management guidance to supporting clients should they have a claim.

We take cyber liability seriously – not only in terms of advising our clients, but also for the business interruption exposure it creates for our business. We never think "it won't happen to us" – as a business that advises on protection, it is even more vital that we focus heavily on internet and data security.

We are also third generation insurance brokers and are proud of our reputation, we take every measure possible to ensure our systems and data are safe – this is a board-level issue. We hold a lot of data and increasingly, this is being used on a variety of mobile devices.

To ensure we were doing all we could to protect ourselves, we brought in an external consultant to examine our processes and staff training. We work with Agenci Information Security, who we knew would take an objective approach.

Agenci helped us realise how much of what we held was our intellectual property – for example, our CRM databases, our pricing structures and business plans and statistics.

These are valuable assets and the risk in terms of loss of profits could be substantial. We were able to re-evaluate our business interruption limits following our work with Agenci and believe the business impact analysis we conducted jointly has proved invaluable.

Potentially, these risks could be as great – if not more so - than physical ones such as fire or flood.

Agenci looked at the way our people operate systems and in terms of data, how we use this, access it, store, transmit and where appropriate, destroy it. We know we cannot be complacent and we felt investing in this service was well worth it – in fact what we have learnt, will also help us in advising our clients.

We have now created a contingency plan that we have tested. We have rigorous processes to back up data and ensure all employees are well trained in their responsibilities.

For example, email disruption could have serious consequences; we are heavily reliant on this. We have also looked closely at our web security, at encryption and how we would operate following a breach.

Payment systems have been scrutinised and we also make sure that our employees understand data regulations – and they can explain if necessary to customers what steps we take to keep their information safe. We hope a crisis never occurs, but if it does, we must be ready.

Our work is ongoing and Lockyer is now working with Agenci to achieve ISO27001 certification, the international standard for information security – this ensures we keep this at the top of our agenda and will provide additional reassurance for clients.

www.theagenci.com
www.lockyers.co.uk

LOCKYERS intelligentinsurance

TOP 8 SECURITY VULNERABILITIES

In June 2014, the Information Commissioner's Office ("ICO") published a report on the top 8 most common security vulnerabilities identified during their investigations of data breaches and how these can be counteracted. Many of these incidents resulted in ICO fines. The breaches could have been avoided if the standard industry practices highlighted in the report were adopted.

The report is aptly named, "Learning from the mistakes of others". Although the report does not have legal effect, if an organisation suffers a breach because it did not follow the guidance in the report, such non-compliance might be considered by the ICO when rendering a decision on sanctions. Companies should therefore ensure that whoever is responsible for their data protection and IT security, has considered the guidance in the report.

1. Software Security Updates.

Attackers search for un-patched, out-dated or otherwise vulnerable software to attack. You should have a software update policy in place for all hardware, including laptops and other mobile devices. You should only use software for which updates are still being provided.

2. SQL Injection.

"Structured Query Language" is a type of programming language designed for database driven software. An SQL injection is a hacking technique which exploits flaws in the programming code. You should consider periodic independent security testing to identify programming issues, including SQL injection flaws.

3. Unnecessary Services.

You should only run network services that are absolutely necessary and ensure that services intended for use on local networks only are not made available to the internet. This will reduce the number of ways an attacker might compromise systems on the network.

4. Decommissioning of Software or Services.

When old or temporary hardware, software or networked services (e.g a website/file server) are no longer needed, you must decommission them and thoroughly check that the decommissioning procedure has actually succeeded.

5. Password Storage.

The report explains "Hashing" and "Salting" techniques which increase the security of stored passwords. Users should also be advised to choose strong passwords (long passwords using a wide range of characters).

6. Configuration of SSL or TLS.

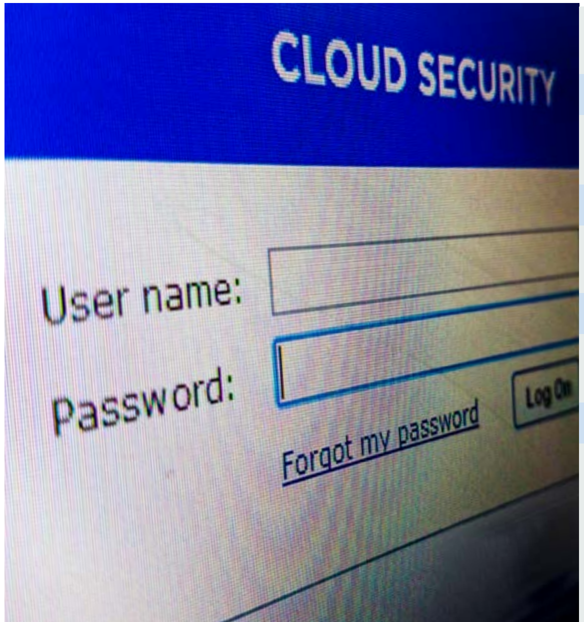
Ensure that personal data (and sensitive information generally) is transferred using SSL (Secure Sockets Layer) or TLS (Transport Layer Security) which are encryption schemes used for ensuring secure communications across the internet.

7. Inappropriate locations for processing data.

Make sure you have policies for all your IT infrastructure for how, when and where personal data will be processed and stored. Apply specific access restrictions where necessary. Ensure that your network has regular back-up and business continuity functions in place.

8. Default credentials.

Change any default credentials provided by hardware and software suppliers, such as standard usernames and passwords, as soon as possible.



Weak passwords

123456	111111
123456789	1234567
1234	1
password	1234567890
12345	00000
12345678	123123
admin	123

Taken from Trustwave's 2014 Global Security Report and their investigation of a cache of passwords stolen by the Pony botnet
www.trustwave.com/gsr

Government Initiatives:

CYBER ESSENTIALS AND CiSP

Cyber Essentials Scheme

In 2012, the UK Government launched "10 Steps to Cyber Security" which encouraged organisations to take steps to manage their cyber risks. The Government has worked with industry to develop the Cyber Essentials Scheme, which covers the basics of cyber security in an organisation's IT system. Implementation of these controls can significantly reduce the risk of common but unskilled cyber-attacks.

Cyber Essentials focuses on internet based attacks, concentrating on five key controls:

1. Boundary firewalls and internet gateways
2. Secure configuration of systems
3. Access control
4. Malware protection
5. Patch management

CYBER ESSENTIALS

Given the media attention surrounding data breaches, it is increasingly important for organisations to demonstrate to clients that they are secure. The Cyber Essentials Assurance Framework is designed to allow third parties to distinguish between organisations that are implementing basic cyber security controls from those that are not.

There are two levels of certification, Cyber Essentials, and Cyber Essentials Plus. The first is awarded on the basis of a verified self-assessment and offers a basic level of assurance which can be achieved at low cost. The second requires external testing of an organisation's cyber security approach, providing a higher level of assurance but at a greater cost. Organisations will need to maintain and develop their cyber security regularly and, as a minimum, recertify at least once a year.

Of course, compliance with the scheme is no 'silver bullet' and many organisations, particularly those who hold vast amounts of information, will need to have far more controls and procedures in place to manage the risks they face. Compliance with Cyber Essentials is a positive first step on the road to better cyber security. More information can be found at:

www.gov.uk/government/publications/cyber-essentials-scheme-overview

Cyber-security Information Sharing Partnership (CiSP)

Cyber-attacks are a threat to all businesses today and insurance companies are particularly attractive sources of information to a range of parties. Commercial data, IP information and sensitive client data are all targets for would-be hackers.

The timely sharing of information about cyber threats is crucial in addressing this issue. The Cyber-security Information Sharing Partnership (CiSP), a joint government/industry initiative established in March 2013, facilitates the sharing of timely cyber threat and vulnerability information on a secure and dynamic environment allowing members to increase their situational awareness and, where necessary, take preventative and responsive measures to protect their business.

A crucial part of the CiSP is a team of government and industry analysts who form the 'Fusion Cell'. This team collate and examine information and data from a number of sources - including threat intelligence reports from government (not publicly available) providing enriched contextual cyber threat and vulnerability information and advice – with the aim of helping organisations better protect themselves.

CiSP recently migrated into CERT-UK where it benefits from being co-located with teams responsible for incident handling and engagement both nationally and internationally. Membership continues to grow with in excess of 550 organisations and 1500 individuals now members of the CiSP (as at Summer 2014) and this growth is projected to continue.

For full details on the joining criteria and process please visit **www.cisp.org.uk**

CiSP

A CATALYST FOR COLLABORATION

ISO 27001

ISO 27000 is a series of information security standards published by the International Organisation for Standardisation. First published in 2005, the ISO 27001 standard outlines how a company can implement an information security management system (ISMS) which can be certified and audited. In September 2013, the ISO 27001 standard was updated to reflect changes in technology, including the rise of ‘bring-your-own-device’ and IT outsourcing to the ‘cloud’.

Whilst the standard focuses on information security, certain required measures will assist organisations enhance their wider cyber-security. The standard not only emphasises the need for robust firewalls, the latest anti-virus software and encryption, but also recognises the need to train employees and implement adequate systems and processes in a coherent and strategic way.

Accreditation is a detailed process; organisations must go through a three-stage external audit process, part of which involves regular ongoing audits to ensure continuing compliance. The process provides a detailed and rigorous method for organisations to plan their information security in a strategic and comprehensive manner which will in turn enhance their cyber-security.

Advice for brokers

The growing number and sophistication of cyber attacks is threatening to outstrip our efforts to increase resiliency against them.

Data breaches are today’s top concern and a serious risk, but governments and forward-looking organisations need to take a holistic view and look beyond these issues to broader risks, including the increasing danger of global shocks initiated and amplified by the interconnected nature of the internet.

In the future, disruption to the internet, as a result of failure or cyber-attacks, will be of such frequency and intensity that most organisations will have to suffer through them as they do natural disasters. The main hope for companies therefore is resilience, the ability to bounce back from disruptions to make them as short and limited as possible.

The following are key issues for brokers to be aware of:

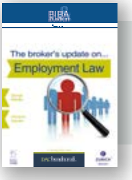
- **Redundancy:** A resilient organisation needs redundant power and telecommunications suppliers, alternate ISPs connected to different peering points, and work-arounds with little reliance on IT to provide alternatives during internet disruptions.
- **Incident response and business continuity planning:** Having trained teams ready to respond when the worst happens is an overlooked strength. Those teams should understand the organisations’ various business lines and most business-critical and time-sensitive information and systems and have defined standard operating procedures based on metrics such as how much time it takes to detect an incident or intrusion, how much time to eject the intruders from the system.
- **Scenario planning and exercises:** The best organisations examine the most likely and most dangerous cyber risks and exercise their security and response teams, as well as their corporate executives and boards, to build muscle memory for responding to incidents.

These recommendations will help insulate organisations from the larger dangers of cyber shocks and while it will be impossible to avoid every shock, organisations should seize the opportunity of each crisis to create ‘teachable moments’ for responders and executives.

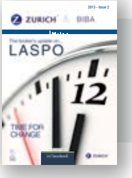
Extract from ‘Beyond data breaches: global interconnections of cyber risk’, a report co-written by the Atlantic Council and Zurich. A full copy of the report can be viewed at http://knowledge.zurich.com/cyber-risk/cyber-risk/

ZURICH®

Other guides in this series are available from the BIBA website – **www.biba.org.uk**



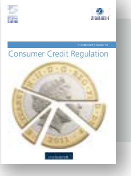
Employment Law



LASPO

Advertising, marketing and branding

Claims



Consumer Credit Regulation

Cyber risks: Data Protection

British Insurance Brokers' Association
8th Floor
John Stow House
18 Bevis Marks
London
EC3A 7JB

Find a broker helpline: 0870 950 1790
Member Helpline: 0844 77 00 266
Fax: 020 7626 9676
enquiries@biba.org.uk
www.biba.org.uk