Protecting your business from cyber crime and data loss

November 2014

Foreword

Today's business environment moves at a rapid pace with a growing reliance on technology, social media and the internet to manage costs and maintain market advantage. This brings with it emerging risks that could result in lost revenue, business down time and a host of unforeseen costs and legal liabilities.

32% of businesses in the UK are more concerned about the threat of cyber crime and data loss now than they were just six months ago[1]. Undoubtedly this has been exacerbated by high profile viruses such 'Heartbleed' and well publicised cyber attacks against institutions like JP Morgan and brands like Tesco.

With the cost of cyber crime estimated to be in the region of £27 billion a year in the UK[2], what can businesses do to protect themselves? In the following report, we consider the various forms of data breach, which businesses are more susceptible and provide practical risk management advice. We also consider the changing legal landscape and what this will mean for companies. Finally, we provide a guide to the insurance cover available and how this can be evaluated to ensure that businesses have the most appropriate level of protection.

James Tuplin
Porfolio Manager TMT
QBE

[1] QBE Business Risk Sentiment Survey June 2014
[2] The Cost of Cyber crime, Cabinet Office 2011

Malicious intent or otherwise

Often, when we think of cyber and data security, we associate any breach with malicious behaviour, and generally an external attack. While such activity is certainly prevalent and indeed on the increase, the loss or breach of data can also be the result of innocent human error or system failure of an internal asset. The impact of this can be no less detrimental.

Irrespective of the cause, when it comes to a data breach, the ramifications can be broad and very costly. The Information Commissioner's Office (ICO) is tasked with upholding information rights in the public interest and is able to levy fines of up to £500,000 per data breach. This is just the tip of the iceberg in terms of consequences; businesses that lose data also have to contend with the reputational damage of such incidents, the impact of business interruption and the cost of notification and rectification. In a recent study, involving 36 large organisations in the UK, the average cost of cyber crime was calculated to be £2.99 million per annum, with each company the victim of just over one successful cyber attack every week[3].

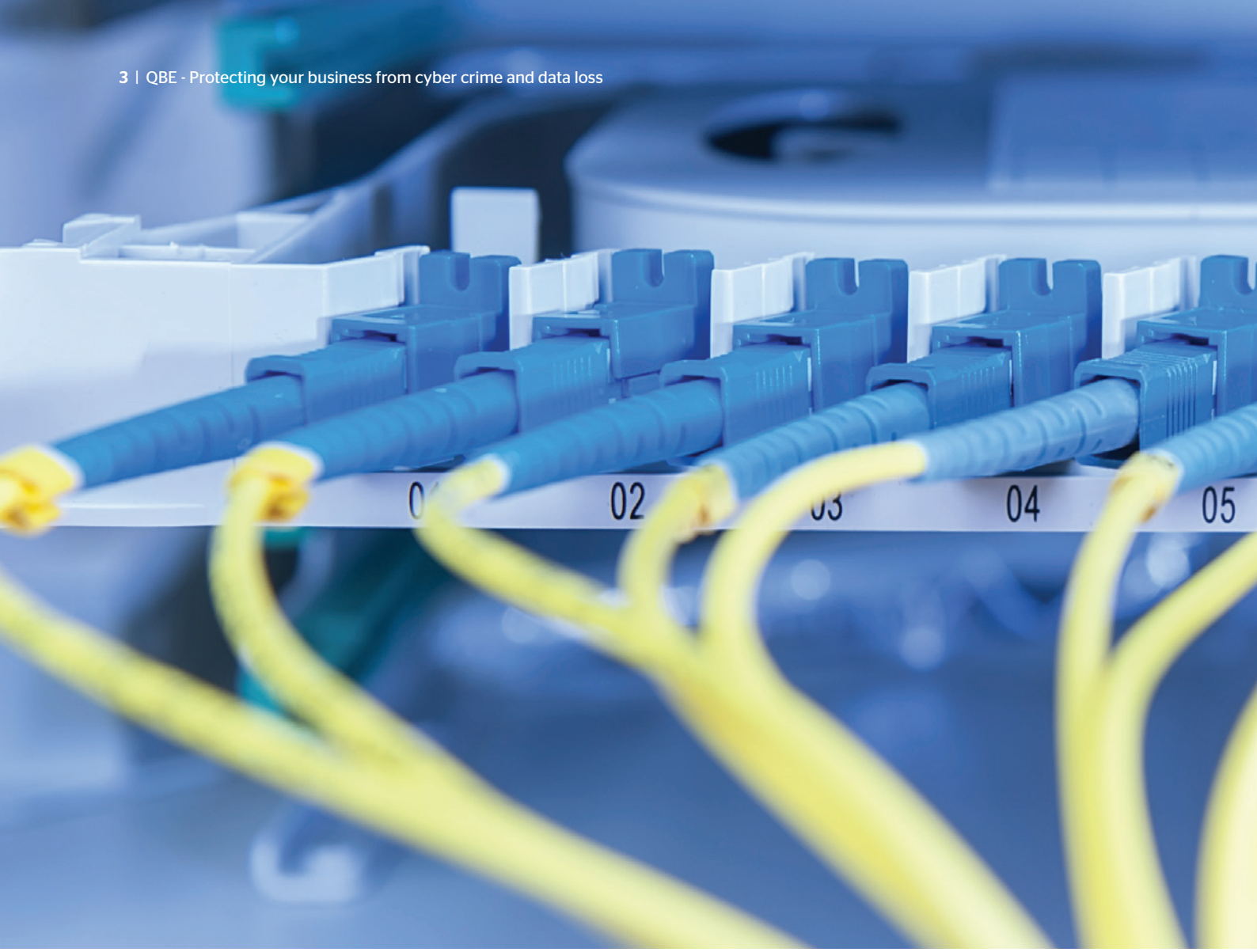
Main types of cyber crime

- Virus or malicious software infection
- Phishing
- Denial of service attacks
- Unauthorised network access by outsiders/employees
- Intellectual property/confidential data theft.

Main cause of data breach

- Malicious or criminal attack
- System glitch
- Human error.

[3] Ponemon Institute UK Cyber Crime Report 2013



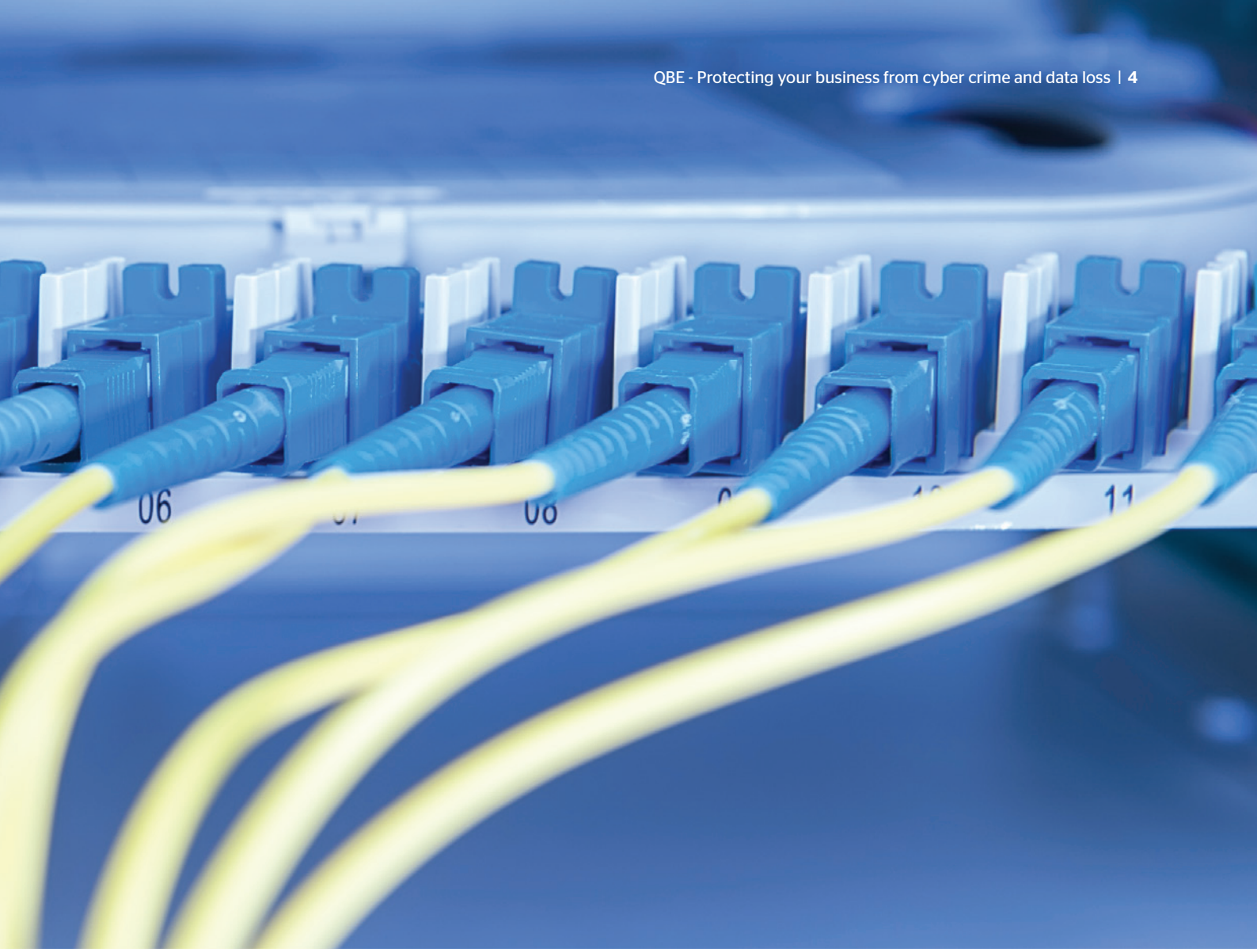
Is my business safe?

With the use of technology so prevalent today, it would be difficult to imagine a business that could consider itself entirely safe from cyber attack or data breach but undoubtedly some businesses are more susceptible than others. Organisations that carry lots of data can be more of a target, particularly when that information is of a sensitive nature or has financial value, such as credit card details or health insurance records. Equally, businesses that trade online are more prone to attack as they have financial data and a higher web presence.

Similarly, those that are connected to more controversial activities, such as animal testing or energy supply, are more of a target due to their particular political/environmental leanings. There have been cases of cyber backlash against organisations as a result of their commercial strategies, for example Apple was attacked in the US over its exclusive agreement with AT&T as sole network provider for its iPhone.

There is a more recent trend for smaller businesses to be targeted. This is largely due to less robust control measures, but also because those businesses can be used as a conduit for something bigger. For example, if a small business has a contract with a much larger organisation, which allows them network access to the larger organisation's data, hackers may target the smaller business as a route into the larger one.

> “Organisations that carry lots of data can be more of a target, particularly when that information is of a sensitive nature or has financial value, such as credit card details or health insurance records.”



How can I defend my business?

Effective risk management will go a long way to protecting a business. Business leaders, or those tasked with the function of risk management, need to first understand their exposures before they can put in adequate controls. Risk management is a continuous process that at no point can be considered complete. As an example, GCHQ provide the following advice:

Ten steps to reducing your cyber risk [3]

1. Home and mobile working – develop an out of office working policy and train staff appropriately
2. User education and awareness – produce user security policies covering acceptable and secure use of your organisation's system and train your employees in them
3. Incident management – establish an incident response and disaster recovery plan, train employees appropriately, test and refine. In a real situation, report criminal incidents to law enforcement
4. Information risk management regime – establish an effective governance structure and determine your risk appetite. Senior level endorsement is essential
5. Managing user privileges – limit user privileges and monitor user activity
6. Removable media controls – control access to removable media and scan all media for malware before importing on to your own system
7. Monitoring – establish a monitoring strategy and continuously monitor ICT systems for unusual use
8. Secure configuration – apply security patches and ensure that the secure configuration of ICT systems is maintained
9. Malware protection – establish anti-malware defences and scan for malware across the organisation
10. Network security – manage your network perimeter and filter out unauthorised access and malicious content.

[3] GCHQ 10 Steps to Cyber Security

Cyber essentials

In a bid to promote a safer online trading environment in the UK, the Government launched the Cyber Essentials Scheme in 2014, which is designed to serve as a 'kite mark' of security for those businesses who undertake a cyber risk review. Businesses that are awarded a Cyber Essentials certificate will be those that can demonstrate that they have basic security measures in place to protect themselves and their customers from internet based threats. Cyber Essentials is applicable to all organisations irrespective of size or activity.

The Government has established a network of approved Certification Bodies, which are independent risk review specialists who work with businesses to verify their self assessments based on five key risk management controls:

1. Boundary firewalls and internet gateways – ensuring devices designed to prevent unauthorised access to or from private networks are effective
2. Secure configuration – ensuring that systems are configured in the most secure way
3. Access control – ensuring appropriate system access for people
4. Malware protection – ensuring that virus and malware protection is installed and up to date
5. Patch management – ensuring the latest supported version of applications is used and all necessary patches supplied by the vendor have been applied.

Once the Certification Body is satisfied that an organisation has implemented the appropriate controls, the Cyber Essentials certificate will be awarded. The Cyber Essentials badge sends a clear message to your clients that you take data security seriously, making you a more attractive trading partner, and can positively impact your risk profile when you come to purchase insurance.

A look at legislation

It has been on the horizon for a number of years but the general consensus is that the European Commission's General Data Protection Regulation (GDPR) will come into force in 2015 with a transition period of two years. Essentially, it will create a single set of rules around data protection that all businesses operating in member states must adhere to. Consultation is still taking place with regard to what the final regulations will contain, but some of the changes mooted include more stringent deadlines for reporting data breaches and greater fines for those breaches. Currently, the GDPR will cap fines at 5% of a company's global turnover or 100m euros, whichever is greater. Whenever the legislation does come into effect, it will be a complete game changer in terms of the responsibilities businesses in the UK will have around data protection. Similar laws have been introduced state by state in the US since the early 2000s and caught many businesses unawares ultimately leading to a meteoric increase in demand for cyber liability insurance.

Risk transfer: what are the options?

Adequate and up to date risk management controls are, without question, essential for all businesses and provide considerable protection against malicious and non-malicious activity. When things do go wrong however, there are insurance policies that offer that added layer of protection. Cyber liability is a relatively new insurance offering in the UK and as a result there are many misconceptions about what is covered and what is not. With the range of policies available, with varying degrees of commonality, insurance buyers must be circumspect in the cover purchased to ensure that it will respond effectively to their particular needs.

A good Cyber Liability policy should include the following:

- Comprehensive 1st and 3rd party cover; sometimes cover in the form of an extension to an existing policy is a poor substitute for a stand-alone policy.
- 1st party cover to include:
  - Notification costs – businesses may be obliged to notify all persons whose data has been compromised. Deadlines for such notifications are likely to become tighter when the new European legislation comes into effect
  - Credit monitoring costs – for the individuals whose credit card data has been lost
  - Forensic costs – to understand what went wrong
  - Business interruption costs – specific for non-physical damage
  - PR costs – to manage the reputational impact of a data breach
  - Service providers – be sure that your policy protects against the loss of your data by one of your service providers
  - Non-targeted attack – some polices will only protect against attacks that have directly targeted your company. Be sure that your cover does not include this restriction.
  - Extortion – which covers your business against ransomware and extortion from a hacker
  - Internal error – not all data breaches are due to malicious behaviour, yet some policies only provide cover for this. Be sure your policy covers you for internal error
- 3rd party cover to include all third party liability in relation to the cyber event (whether an attack or a data breach) with cover for damages, invasion of privacy, libel, slander and defamation.

You think you are covered?

As UK businesses adjust to the threat of cyber attacks and data breaches, there are a few common misconceptions about cover to look out for. The following will not provide adequate cyber cover:

- Compulsory professional indemnity policies: these may include a degree of 3rd party cyber liability cover but usually will not cover 1st party costs
- Cyber extensions to General Liability, Professional Indemnity or Directors' & Officers' cover: these will generally only provide basic 3rd party cover and again may not cover 1st party costs levels of cover either, it is much better to have a stand alone Cyber Liability policy
- Business interruption as part of a Property policy – this will not cover for non-physical damage

Where to go for further information

The Government has produced a series of guides to help businesses understand cyber threats. The most useful reports can be downloaded here

10 steps to cyber security

www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

Cyber Essentials Scheme

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

QBE's Cyber & Data Security offering

Cover is provided on a 1st and 3rd party basis and includes:

- Breach of privacy – including call centre support for your customers when you suffer a breach
- Breach of intellectual property rights
- Business interruption
- Cyber extortion and forensic support
- Claims support by a dedicated and specialist Crisis Management team – which includes a 24/7 hotline.

For more information, contact our Technology, Media and Telecommunications team on +44 (0) 20 7105 4000 or at TMT@uk.qbe.com. Alternatively, visit **www.QBEeurope.com/cyber**

About QBE

QBE is a business insurance specialist. We understand the risks businesses face and support organisations from a diverse range of sectors in managing and mitigating their risk enabling them to realise their objectives.

An A+ rated insurer, we have the appetite and capacity to provide cover for businesses of all sizes.

Our extensive product range includes:

Accident and health (inc commercial PA and business travel)	Pharmaceutical and medical
After the event insurance	Political risk and terrorism
Commercial crime	Product guarantee and recall
Commercial combined	Product protection
Contractor all risks/EAR	Property
Energy, offshore and onshore	Reinsurance
Entertainment and leisure industry	Scheme underwriting facility
Environmental impairment liability	Specie
Financial and professional liability (Cyber Liability, Director's & Officer's, Professional Indemnity)	Surety/bonds
General liability (Employer's Liability, Public Liability, Tradesman)	Trade credit
Marine	Warranty and GAP
Motor Commercial (inc fleet, haulage, bus and coach, motor trade)	

Risk management

Effective risk management is a feature of all successful organisations – and it's one of our key underwriting considerations. We work closely with businesses to improve their systems and processes; minimising their exposure to risk and helping to reduce the frequency and severity of any losses.

We stand by our claims

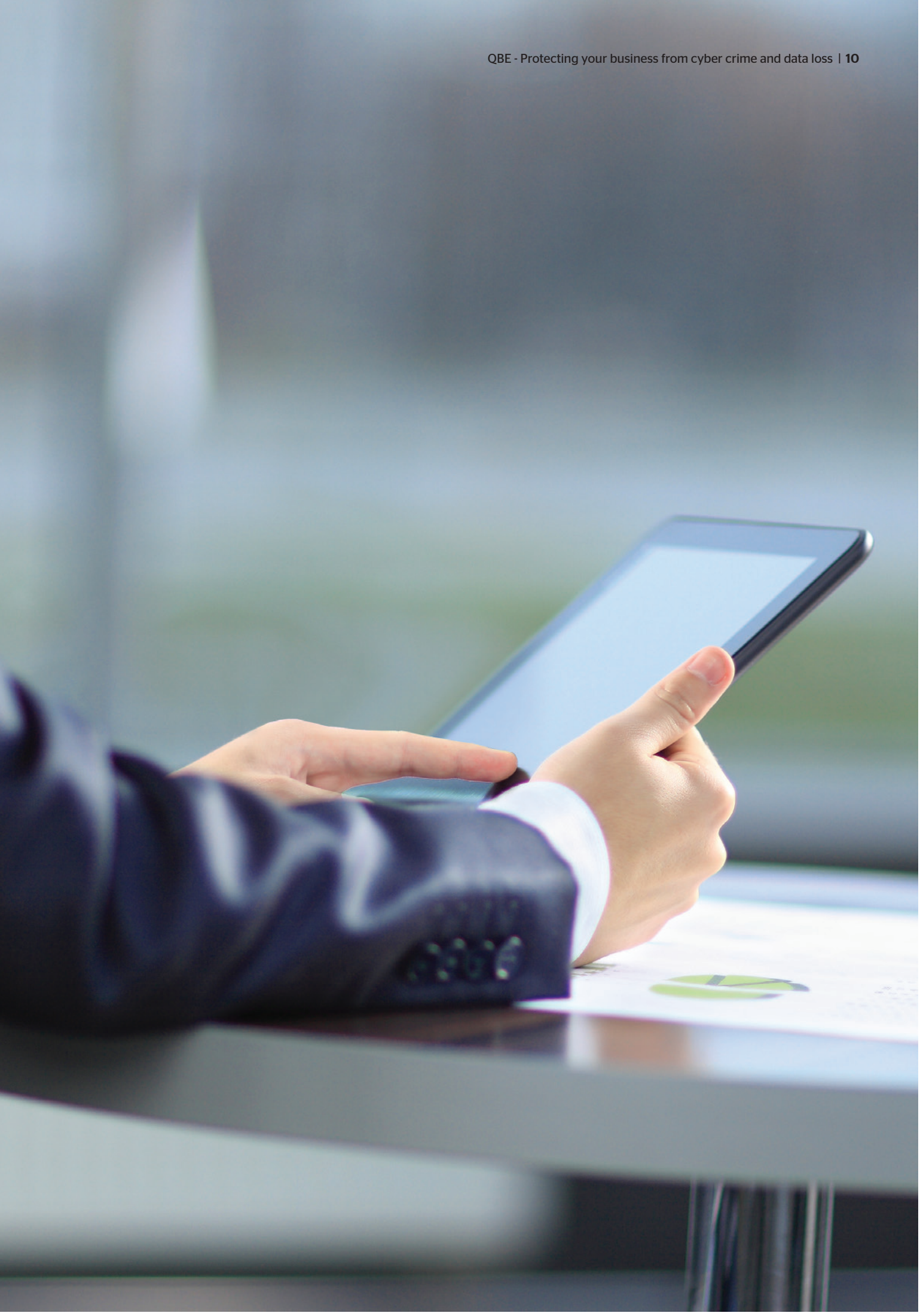
Inevitably, claims do occur. That's when businesses really discover the value their insurance company delivers. We pride ourselves on our positive attitude and proactive approach to claims management. Our claims teams have a deserved reputation for the professional, efficient and sympathetic way they work with brokers and clients when losses are incurred.

Local knowledge

UK underwriting offices: London, Belfast, Birmingham, Bristol, Chelmsford, Glasgow, Leeds, Manchester and Stafford.

To find out more

For more information about QBE and how we can help your business, please visit our website **www.QBEeurope.com**



QBE European Operations

Plantation Place, 30 Fenchurch Street, London EC3M 3BD

tel +44 (0)20 7105 4000
www.QBEeurope.com

xxxxGC/CYBERREPORT/OCT2014