KING & SPALDING

Client Alert

Corporate Practice Group

June 19, 2014

UK Cyber Security Guidelines

The UK Government has issued details of its Cyber Essentials Scheme to assist organisations with their cyber security measures.

The scheme allows organisations to apply for one of two levels of cyber security "Badge" certification :

- Cyber Essentials – requires organisations to complete a self-assessment questionnaire (to be marked by an independent external body); or

- Cyber Essentials Plus – the organisation's systems are tested by an independent external body.

Obtaining and marketing the cyber security badge should demonstrate confidence in that organisation's cyber security measures to consumers and the public. The cost of obtaining a badge will depend on the certifying body.

The Cyber Essentials Scheme documents can be downloaded at:

https://www.cyberstreetwise.com/cyberessentials/#downloads

Cyber Security Directive and General Data Protection Regulation

Additionally, the new Network and Information Security Directive, known as the Cyber Security Directive, sets out cyber security requirements applicable to certain market operators and information system providers. It is likely to come into force in 2015 or 2016. European countries will need to implement legislation to give effect to this Directive which can take up to an additional two years. There are also similar obligations to take security measures for all organisations which process personal data under the new General Data Protection Regulation which is also expected to come into force in 2015 or 2016 (and will be directly effective soon after, without the need for each European country to implement local legislation). A breach of the General Data Protection Regulation can expose the organisation to a potential maximum fine of the greater of EUR 100 million or 5% global turnover.

Cyber Essentials Scheme

The scheme focuses on internet-originated attacks against an organisation's IT system (recognizing that many organisations will need to implement cyber

For more information, contact:

Pulina Whitaker
+44 (0)20 7551 7586
pwhitaker@kslaw.com

King & Spalding
London
125 Old Broad Street
London EC2N 1AR
Tel: +44 20 7551 7500
Fax: +44 20 7551 7575

www.kslaw.com

security measures for the other services they provide). Organisations should conduct cyber security risk audits and take steps to mitigate against these risks.

The five key controls (identified by CESG, the information security arm of GCHQ) of the Cyber Essentials Scheme are:

1. Boundary firewalls and internet gateways;

2. Secure configuration;

3. Access control;

4. Malware protection; and

5. Patch management.

The Government believes that organisations can mitigate against the damage caused by cyber attacks and reduce the risk of a phishing or hacking attack if they implement Cyber Essentials and also continually review their cyber security risks.

Key cyber threats

The key cyber threats facing organisations are:

- State-sponsored hackers – to obtain corporate confidential information, trade secrets or intellectual property or to cause damage through sabotaging critical infrastructure;

- Organised criminals – to obtain personal identification or payment information to steal monies or commit fraud;

- Hacktivists – for perceived status or kudos from the hacking communities or for social or political ideologies;

- Organisations – to obtain corporate confidential information, trade secrets or intellectual property for competitive advantage or to sell to competitors;

- Current or former employees – for financial gain or for grudge-related reasons.

The specific cyber threats for a particular organisation will depend on the nature of its business and the type of information held by it. Organisations should also consider taking out insurance cover to reduce the financial consequences of a cyber attack.

What to do if an organisation is cyber attacked

The key to minimising the impact of an attack is detecting it quickly. Many organisations are unaware they have suffered an attack until sometime after the incident, occasionally when sensitive information is published in a blog or a website. As soon as an attack has been detected, organisations should:

1. *Implement an Incident Response Plan*

   Organisations should have an Incident Response Plan ready for when an attack is made. A Technical Incident Response Team should already be primed to step-up and deal with an attack and to implement the Incident

response Plan. The Team should liaise with senior management, shareholders, lawyers and independent cyber experts as necessary being contacted to deal with the attack as soon as possible. The goal should be to minimise any disruption to the business and to maintain consumer confidence.

A forensic analysis of the attack by cyber experts, to determine the scope of the damage and the risk of another or an ongoing attack, should be conducted as quickly as possible. Insurance providers may need to be notified. Lawyers may need to be instructed to safeguard evidence, conduct or assist with internal investigations and prepare to defend the organisation against claims and also to deal with notification obligations (see below).

2. *Comply with notification obligations*

Some European countries have current obligations to notify data protection authorities about personal data breaches (in the UK, only some organisations such as internet service providers and telecommunications operators must notify the UK data protection authority within 24 hours of a breach). After the new General Data Protection Regulation is in force, all European data controllers will have to notify the data protection authority about a breach incident which compromises personal data without undue delay. There are parallel obligations under the proposed Network and Information Service Directive (although internet service providers will now be excluded from this obligation). Other regulatory bodies may also need to be notified. In some instances, individuals whose personal information has been compromised may or should also be notified.

3. *Issue a PR statement and social media messages*

Public statements, across all forms of media, should be issued to reassure consumers and stakeholders, to pre-empt a potential backlash and to regain confidence in the organisation.

Continual review of cyber attack risks

The Government's Cyber Essentials Scheme is a useful starting point for organisations who are only recently, or who have not started, to consider cyber security risks to their businesses. Cyber security professionals view the chances of businesses becoming victims of a cyber attack as being almost inevitable. According to UK Government research, 87% of small firms in the UK experienced a cyber security breach in 2012. 93% of large firms were also targeted. Some incidents caused more than £1 million in damages.

The Cyber Essentials badge certification does not provide a clean bill of health but just confirmation that the organisation's cyber security measures are satisfactory at the time the assessment is conducted. It is crucial that organisations continually review the risks their businesses face, including the structure and make-up of their workforce, geographical operations and the sensitive nature of their business information. Cyber security measures should be review and updated accordingly. The Government recommends that organisations with badge certifications recertify at least once a year to retain the badge. Additionally, there are other cyber security standards which organisations can consider implementing, such as ISO 27001.

* * *