KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

February 5, 2015

UK Government Issues Additional Cyber Security Guidance

The UK Government has issued additional guidance for organisations to help them protect themselves against a cyber attack. The new guidance supplements the previous guidance by setting out what common cyber attacks look like and how hackers typically execute these cyber attacks.

The UK Government's security and intelligence organisation, GCHQ, has stated that cyber attacks do not show any signs of abating. Cyber attacks pose a threat not only to the financial health of an organisation but also to its value, its reputation, the security and privacy of its staff and the confidentiality of its information and trade secrets. Cyber security insurance is becoming increasingly popular but providers often link premiums to the level of cyber security systems and processes. The UK Government has stated that organisations must engage top-level management in the formulation of their cyber security strategies and that pro-active management of cyber risks at Board (or equivalent) level is critical. The responsibility for a cyber attack ultimately rests with the Board or senior management and the UK government is keen to ensure that organisations place cyber security high up on the agenda of management meetings.

Cyber attacks are often from hackers based overseas and a co-ordinated approach with intelligence agencies of other countries is needed to deal with these risks. GCHQ has stated that it "*and MI5*[1] *are working with their US partners to further strengthen UK-US collaboration on cyber security by establishing a joint cyber cell, with an operating presence in each country. Aimed at strengthening mutual cyber defence, it will bring together agencies and law enforcement and allow staff from each agency to be co-located, enabling information and data to be shared at pace and at greater scale*". Following the UK Prime Minister's recent meetings with the US President, a new cyber security envoy, Mr. Andy Williams, has been appointed to help British small businesses and first-time exporters promote their business interests across the US.

For more information, contact:

Pulina Whitaker
+44 207 551 7586
pwhitaker@kslaw.com

Clare Lynch
+44 207 551 7552
clynch@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

Common Cyber Attacks

The new paper from GCHQ deals with the following topics:

1. The Threat Landscape

Typical cyber attackers include:

- cyber criminals intent on profiting from the attack;
- industrial competitors seeking confidential information or trade secrets;
- foreign intelligence services seeking competitive advantages for their countries;
- hackers motivated by the challenge of the attack itself or personal kudos;
- hacktivists acting with political or ideological motives; and
- employees (acting maliciously or negligently).

Cyber attackers use tools and techniques available on the internet, including tools designed for security specialists, as well as bespoke tools and techniques, including malicious code. Attacks can be targeted or untargeted. Organisations should be aware that attacks can come from within the organisation itself, as well as from outside, and effective employee or contractor supervision and monitoring is crucial to prevent or reduce the impact of an attack from an insider.

2. Understanding Vulnerabilities

Vulnerabilities provide opportunities for attackers to gain access to an organisation's systems and can occur through flaws, features or simple user error. There is now a market for acquiring information about the "zero-day" vulnerabilities (those which are not publically known) of organisations and these are often used by well-resourced attackers in bespoke attacks.

3. Common Cyber Attacks - Stages and Patterns

GCHQ has summarised the four main stages of a cyber attack:

- survey: investigating and analysing available information about the target to identify vulnerabilities such as using scanning tools to identify any open ports, open services, default settings and vulnerable applications and operating systems;

- delivery: reaching the point in a system where a vulnerability can be exploited such as sending an email with a virus or a link to a malicious website, distributed infected USB sticks or creating false websites for the public to gain security information;

- breach: exploiting the vulnerability to gain access such as making changes to the operating system, gaining access to online accounts or controlling a user's computer or device; and

- affect: carrying out the activities within the system to achieve the intended goal of the attacker such as establishing a presence within the system or controlling an administrator's account to obtain information or make changes for financial gain or destructive effect.

4. Reducing Your Exposure to Cyber Attacks

Putting in place robust security tools and internal security processes, including training all personnel who use the IT systems, can reduce the risk of an attack using tools and techniques available on the internet. Additionally organisations should have:

- established network perimeter defences such as web proxy, web filtering, internet gateways and firewalls to detect and block non-business downloads;
- malware protection;
- patch management;
- secure configuration and restriction of functionality of devices to they are limited to business use only;
- robust password policies; and
- restricted user access controls.

5. Case Studies

The case studies demonstrate how attacks can be used to gain access to organisations' confidential information and trade secrets.

Steps to take now

Board-level (or equivalent senior management) engagement on cyber security issues is highly likely to be critical for an organisation to reduce the impact of a cyber attack. An initial risk assessment should be undertaken to determine the level and extent of such risks. The majority of organisations are likely to be attacked at some point because of the prevalence and the relatively broad nature of the threat landscape. Organisations should take preventative steps to deal with cyber risks as early as possible. Undertaking a (privileged) security assessment is a key early step to be taken. All staff who have access to IT systems should have refresher training in keeping the systems secure, tailored to regular reviews of the cyber threats facing that organisation. Having cyber security insurance is also recommended. A strategy should be formulated according to the level and extent of the relevant risks. Having an incident response plan will be key to tackling a cyber attack quickly. Additionally, organisations should have in place well documented and accessible plans to engage legal, forensic and PR teams which can be triggered as soon as an attack is registered.

* * *

Celebrating more than 125 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 800 lawyers in 17 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality and dedication to understanding the business and culture of its clients. More information is available at www.kslaw.com.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered "Attorney Advertising."

[1] The UK's nationals security service.