Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 14, NUMBER 6 >>> JUNE 2014

New U.K. Guidance on Online Personal Data Protection, Cloud Services and the Amorphous Cyber Threat

By Steven James, of Brown Rudnick LLP, London.

Another day, another cyber attack.

As this article was being written, the U.K. National Crime Agency warned of a "powerful cyber attack" to hit U.K. computers within the next two weeks[1] . Reported in much the same manner as an incoming tornado or swine flu pandemic, it is the latest in a series of cyber threats to nations, businesses and individuals. We had barely got over the news that eBay's security systems had been compromised, forcing 230 million people to change their eBay passwords, and giving eBay a considerable public relations headache. And before this there was the Heartbleed bug, which threatened to expose OpenSSL encryption software, used by a multitude of online providers (including popular social media sites like Facebook). Again, the result was that millions of users had to change their passwords.

The consequences to businesses of a cyber attack can be devastating. A business which is the victim of a cyber attack may find itself on the wrong end of a breach of contract or negligence claim (including potentially from its own customers) for failing to take reasonable precautions when storing customer or corporate data. Whilst a carefully worded *force majeure* clause might catch the likes of a Heartbleed attack, it will probably not come to your aid in other circumstances where you have simply failed to take adequate steps to protect your systems. Although it may be financially, practically and legally difficult for customers to bring a breach of contract or negligence action, particularly given the likely broad exclusions in the service provider's terms, the business's suppliers and commercial customers, with negotiated contracts and more resources, may well be in a stronger position to bring a claim. Listed and regulated companies may also find themselves in breach of obligations to take reasonable steps to establish and maintain adequate procedures, systems and controls to counter cyber attacks, and may be obliged report the loss of price sensitive information.

The loss or theft of data in the U.K. could also trigger obligations to notify the Information Commissioner's Office (ICO). The ICO has the power to issue fines of up to 500,000 pounds (U.S.$848,040) against data controllers (which will include the majority of online service providers) who fail to take sufficient steps to protect personal data. Whilst fines of such magnitude are rarely handed out in practice, and may not do too much damage to a company the size of eBay, or indeed Sony — which was fined 250,000 pounds (U.S.$424,020) by the ICO in January 2013 for failing to install up-to-date security software, which in turn was held to have led to the hacking of personal data, including card details and personal details, of millions of

customers (*see analysis at WDPR, February 2013, page 7*) — the reputational damage can be cataclysmic. Trust on the Internet, particularly e-commerce sites, is everything. Further, if the mooted fines of up to 5 percent of annual global turnover (rather than 2 percent as originally proposed) or 100 million euros (U.S.$135.4 million) (if greater), are introduced for data breaches under the proposed EU General Data Protection Regulation to replace the EU Data Protection Directive, this could severely hit the bottom line of even the most successful global businesses.

Cyber attacks are therefore an almost amorphous threat with the potential to wreak havoc.

But what can be done to combat the threat, particularly where personal data and third party cloud services are concerned?

Two recent publications from the ICO and the U.K. Communications-Electronics Security Group offer guidance on how to mitigate these threats.

The ICO Guidance

There are no simple answers to cyber attacks, but steps can be taken to mitigate the threat. Indeed, the ICO has attempted to calm fears by offering practical measures to combat cyber attacks and, in particular, to help businesses comply with the seventh data protection principle under the U.K. Data Protection Act 1998. The seventh data protection principle requires the data controller to ensure it has implemented adequate technical and organisational measures in order to protect against the unauthorised or unlawful processing of personal data and the accidental loss or destruction of, or damage to, personal data. This is a broad and generalised obligation, and is likely to require an integrated patchwork of measures to ensure compliance, particularly where online services are concerned.

In its 47-page data security report, "Protecting personal data in online services: learning from the mistakes of others"[2] , issued in May 2014, the ICO offers best practice advice on how to avoid eight common pitfalls which lead to data security breaches, namely: a failure to keep software security up to date; lack of protection from Structured Query Language injections; use of unnecessary services; poor decommissioning of old software and services; insecure storage of passwords; failure to encrypt online communications; poorly designed networks processing data in inappropriate areas; and continued use of default credentials, including passwords.

The ICO's proposed recommendations to mitigate the risks associated with these flaws include the following:

Ensure You Have a Clearly Defined Software Security Update Policy and Procedures

Whilst there may be justifiable reasons why security updates cannot be implemented immediately (for example, testing requirements), applying software updates as soon as reasonably practicable upon such updates being made available is critical to ensuring that no vulnerabilities are exposed in the system. Supported software should be used as a matter of course for all the organisation's software components and hardware assets, including laptops, mobile phones and tablets.

Take Steps to Mitigate the Threats of 'SQL' Injections

Structured Query Language (SQL) injections are flaws which introduce coding errors into databases designed to receive information (including personal data). In the most serious cases, SQL flaws can compromise an entire system by executing arbitrary code, with the potential for compromising significant amounts of personal data. In order to mitigate the risk, businesses should ensure that external suppliers are responsible for issuing software fixes/patches to remedy SQL errors in the source code. This should be coupled with internal penetration testing, vulnerability assessments, code reviews and a software coding and updates policy for both externally and internally developed source code.

Avoid Using Unnecessary Systems

The ICO recommends maintaining a list of which services businesses make available, restricting or decommissioning any service that is not necessary (which will depend on the cost-benefit for the business of running each service), whilst avoiding high risk services (like Telnet, plain File Transfer Protocol (FTP) and open mail (Simple Mail Transfer Protocol, or SMTP) relays) and using secure networks such as Virtual Private Network (VPN). All aspects of temporary and legacy systems should be disabled and decommissioned, to ensure that a service is not inadvertently left running and accessible. Systematic port-scanning should be used to check whether they have been decommissioned.

Ensure You Have Secure Password Storage

Passwords are a prime target for hackers, as illustrated by the cyber attacks on eBay. The ICO makes clear that it is vital to have password handling procedures in place before a security breach occurs. If you do not have in-house expertise in password handling, you should consider engaging third party authentication providers. Passwords should not be recoverable directly, or held in plain text, due to how easily they can be read, or in a decryptable form. The ICO instead recommends businesses take the following steps:

- use "hashing", which is a one-way method which converts a password into a hashed value. When a user first registers with a service and provides a password, this is hashed, and only this hash value is stored. When a user attempts to log in and enters his/her password, a hash is generated, and if this hash matches with a stored hash, a secure connection is made. As this is a one-way authentication process, it is very difficult for a hacker to work out which hash matches with which password, even if the hacker has a list of hashes to hand. While a hacker could try to guess the passwords and match these against a list of hashes, this will be extremely time consuming and difficult for a hacker to do. Whilst the hash system is not impenetrable, if you are alerted to a potential se-

   ISSN 1473-3579

curity breach, it should give you time to take steps (such as to reset compromised passwords) before the hacker has any time to guess multiple passwords and fully compromise your systems. The ICO recommends that organisations periodically review the strength of the hash function and keep up to date with technological advancements, as these may lead to some hashing measures no longer being appropriate to secure passwords;

- use a technique called "salting", which is a string of random data unique to each user, increasing the length and complexity of the value that is hashed. The salt is used by combining it with the user's password, then hashing the result. The salt is then generally stored alongside the hash in a database. Using salts further increases the time and effort it will take to crack multiple passwords;

- ensure users create strong passwords, using a wide range of characters, and a combination of upper case letters, lower case letters, numbers, punctuation marks, and other symbols, avoiding the use of dictionary words where possible and simple substitutions, such as "p4$$w0rd", and the use of patterns derived from the physical keyboard layout (*e.g.*, "qwerty" or "1qaz2wsx"). Default credentials and passwords should be avoided. Default credentials are often provided for services such as firewalls, content management systems or administration accounts for a database, and will be an easy target for the hacker that has some indication as to what systems or services an organisation uses; and

- have a plan of action in case of a password breach, which should include how to reset users' passwords in bulk and how to notify users of what has happened and what they need to do about it.

Encrypt Communications

Encryption is vital to ensure that any personal data or sensitive information transmitted will not be viewable via any computer system on the route between the two systems. A connection between two systems using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) ensures that: 1) the communication is encrypted; and 2) the identity of one or both of the end points can be trusted. But the use of SSL and TLS for encryption purposes must be consistent and of sufficient strength. Any included content such as images, JavaScript or Cascading Style Sheets (CSS) should also be provided over SSL or TLS to prevent "mixed content" from compromising security. Users should not be allowed to be able to navigate away from a secure website and then return to it, as hackers will be able to have access to the user's session cookie. All websites covered by the same system should have a valid digital certificate, which is designed to assure the user that the organisation has satisfied a certificate authority that it is legitimately in control of the domain name(s) for which the certificate is issued. Digital certificates should be renewed to ensure the service remains secure. Extended Validation (EV) certificates are available from certificate authorities to provide a higher level of assurance.

Have Robust Security Architecture

Security systems should be well designed so that testing or staging environments are segregated from the production environment, with the network architecture accounting for different functions, such as backups and business continuity. You should regularly ensure that web servers are not exposing private/restricted content.

The Communications-Electronics Security Group Guidance

The Communications-Electronics Security Group (CESG), which is the information security division of GCHQ (the U.K. Government Communications Headquarters) as well as the National Technical Authority for Information Assurance in the U.K., published in May 2014 "Cloud Security Guidance: Risk Management"[3], but this is specifically for businesses using cloud services to store and process sensitive data. The use of cloud services is becoming increasingly common, in part due to the substantial costs savings and efficiencies they can offer. But cloud service providers often offer very little in terms of contractual protection and security for data.

The CESG provides a step-by-step guide to manage the use of cloud services, making it clear that customers need to do more than simply accept assurances from cloud providers at face value. The intention appears to put the onus on customers to decide which services are suitable to handle their data, depending on their assessment of its sensitivity.

Whilst the Cloud Security Guidance is targeted at the public sector, it is equally useful for private businesses.

The Guidance advocates a seven-step approach for risk management when assessing and using cloud services, namely:

1) know your business requirements, considering issues such as availability and accessibility. In the context of those business requirements, you should form a risk appetite by identifying any risks which would be unacceptable to the organisation, should there be a breach;

2) identify the information that will be processed, stored or transported by the cloud service and understand any legal or regulatory implications (including under data protection legislation) that may be incurred as a result;

3) understand which security principles are relevant in conjunction with your business requirements, risk appetite and the information which will be exposed to the service provider;

4) understand which principles the service provider implements and the approach taken to implement them;

5) understand what assurance is available in their implementation (including third party validation);

6) consider what additional mitigations consumers can apply; and

7) consider whether the remaining risks are acceptable.

These practical steps have in turn been informed by, and should be read in conjunction with, a set of 14 Cloud Security Principles[4] the CESG developed jointly with the Cabinet Office. These outline the broad security requirements which the CESG considers are crucial for adequate and robust security risk management, including data in transit protection, separation between consumers, governance, operational security, identity and authentication, secure service administration, audit information provision to consumers and secure use of the service by the consumer.

The CESG has stated that two further parts of its Cloud Security Guidance will be published soon: a consumer guide providing guidance for organisations on how to use a cloud service in the most secure way, and a separation guide which will provide specific guidance on the strength of separation between consumers in cloud services.

Impact on Businesses

Whilst many of the practical steps discussed in the ICO guidance and the CESG guidance will be all too familiar to information technology (IT) professionals, and some of them should be obvious to most people (*e.g.,* running regular software updates and using complex passwords with multiple different characters), they serve as a pointed reminder to businesses of what is required in the current climate. They also give the clearest outline yet of what standards are expected in order to avoid liability and comply with data protection legislation.

The two sets of guidance may also help bridge the gap between what the IT security professionals are saying is required, on one side of businesses, and the priorities and drivers of the commercial directors (focused on the company's bottom line and market growth), on the other. IT professionals and business leaders are going to have to work together to ensure compliance. Their interests, as far as data security is concerned, should be aligned. Data security must be a top priority (if it is not already).

Those engaging cloud services providers are encouraged to take an increasingly proactive approach in order to ensure that the provider and the cloud services are appropriate for their business requirements and risk appetite, whilst data controllers are expected to take an integrated, systematic approach to IT security.

It seems that taking a passive approach to data security in an age of cyber threats will no longer be tolerated by regulators. The unequivocal message is that prevention is better than the cure, and that businesses should help themselves before someone else helps himself to customer or corporate data.

NOTES

[1] http://news.sky.com/story/1274201/cyber-attack-to-hit-in-next-two-weeks.

[2] http://ico.org.uk/news/latest_news/2014/~/media/documents/library/Data_Protection/Research_and_reports/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf.

[3] https://www.gov.uk/government/publications/cloud-security-guidance-risk-management/cloud-security-guidance-risk-management.

[4] https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles.

The text of the ICO report, "Protecting personal data in online services: learning from the mistakes of others", is available at http://ico.org.uk/news/latest_news/2014/~/media/documents/library/Data_Protection/Research_and_reports/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf.

The text of the CESG's "Cloud Security Guidance: Risk Management" is available at https://www.gov.uk/government/publications/cloud-security-guidance-risk-management/cloud-security-guidance-risk-management.

The text of the Cloud Security Principles is available at https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles.

Steven James is Counsel at Brown Rudnick LLP, London. He may be contacted at sjames@brownrudnick.com. The views expressed in this article are solely those of the author and do not necessarily represent the views of Brown Rudnick LLP. Information contained in this article is not intended to constitute legal advice by the author or the lawyers at Brown Rudnick LLP, and it does not establish a lawyer-client relationship.

   ISSN 1473-3579