ROPES & GRAY ALERT

Intellectual Property Transactions

July 10, 2017

Cybersecurity – A Recent UK ICO Fine Provides 60,000 Reasons for Organisations to Review Data Security

Attorneys
Rohan Massey

On 27 June 2017, the Information Commissioner's Office issued a £60,000 fine to a company hit by a cyberattack along with a warning to all SMEs to ensure that they are doing all they can to safeguard their customers' personal details. In its Monetary Penalty Notice to Boomerang Video Ltd, the ICO said that the video game rental firm had failed to take basic steps to stop its website from being attacked, including failure to carry out regular penetration testing and the holding of encrypted cardholder details and CVV numbers for longer than necessary. The ICO considered that, because Boomerang's contravention was serious, had been for "no good reason" and was likely to cause substantial damage and distress, a monetary penalty was warranted under s 55A of the Data Protection Act 1998.

Background

The Boomerang Video website was developed in 2005 by a third-party company ("data processor"). It was unaware that the login page contained a coding error. On 5 December 2014, an attacker exploited this vulnerability by using SQL injection to gain access to usernames and password hashes for the WordPress section of the site.

One password was shown to be a simple dictionary word based on the company's name. The attacker then uploaded a malicious web shell onto the web server to further compromise the system and gain access to the personal data of individuals stored within.

On 30 December 2014, the attacker was able to query the customer database and download text files containing 26,331 cardholder details (including name, address, primary account number, expiry date and security code). Part of the primary account numbers were stored unencrypted and the attacker was otherwise able to gain access to the decryption key with ease, using information in configuration files on the web server. Notably, industry guidelines prohibit the storage of the security code after payment authorisation.

ICO investigation

The ICO found that Boomerang had failed to take basic steps to stop its website from being attacked. In particular, it found that:

- Boomerang had failed to carry out regular penetration testing on its website that would have detected errors;
- the firm had failed to ensure the password for the account on the WordPress section of its website was sufficiently complex;
- it had some information stored unencrypted and the information that was encrypted could be accessed because it failed to keep the decryption key secure; and
- encrypted cardholder details and CVV numbers were held on the web server for longer than necessary.

Serious contravention (s 55A(1)(a))

The Commissioner was satisfied that the contravention itself was serious due to the number of individuals, the nature of the personal data that was stored on the database and the potential consequences. She also said that Boomerang Video's failure to take adequate steps to safeguard against unauthorised or unlawful access was serious.

Substantial damage or distress (s 55A(1)(b))

The ICO noted that the customer database stored financial information and that the attacker accessed 26,331 cardholder details (including name, address, primary account number, expiry date and security code). The personal data that was obtained was clearly of interest to the attacker given the targeted nature of the attack, and some of it was used for fraudulent purposes. The database therefore clearly required adequate security measures to protect the personal data.

The ICO said that for no good reason, Boomerang appeared to have overlooked the need to ensure that it had robust measures in place despite contracting with a data processor that could have carried out the work.

Failure to take reasonable steps to prevent foreseeable risk (s 55A(1)(c))

Rather than a deliberate contravention of the DPA, the Commissioner considered that the inadequacies demonstrated by Boomerang were matters of serious oversight. She considered that Boomerang ought reasonably to have known that there was a risk that this contravention could occur because it was of course aware of the data, including financial, that was stored on the customer database.

The ICO also said that SQL injection is a well-understood vulnerability and known defences exist. She added that Boomerang ought to have known that it would cause substantial damage or substantial distress to the data subjects if the information was accessed by an untrustworthy third party who would expose them to fraud.

The ICO said that in these circumstances, "reasonable steps" would have included carrying out regular penetration testing on the website and correcting the SQL injection vulnerability, ensuring that the password for the WordPress account was sufficiently complex, and keeping the decryption key secure.

Decision to impose fine

The Commissioner considered that there was no good reason for Boomerang's catalogue of failures. She considered that there was a serious contravention of the seventh data protection principle with respect to the personal data that was stored on the customer database. The contravention was of a kind likely to cause substantial damage and substantial distress, and Boomerang knew or ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention. As such, the conditions for issuing a monetary penalty under s 55A were met.

Additionally, the Commissioner said that she did not believe that the contravention could be characterised as a one-off event or attributed to mere human error.

Mitigating features

The Commissioner took into account the following mitigating features of the case:

- Boomerang's website was subjected to a criminal attack.
- Boomerang reported this incident to the Commissioner and was cooperative during her investigation.
- The data processor had assured Boomerang that the payment security codes were not stored on the customer database.
- Boomerang has now taken substantial remedial action.

- A monetary penalty may have a significant impact on Boomerang's reputation (and to some extent) its resources.

Aggravating features

The Commissioner took into account the following aggravating features:

- Boomerang was not aware of the security breach until 9 January 2015 (over a month after the attack) when it was notified by its customers.
- Boomerang assessed itself to be compliant with the "Payment Card Industry Data Security Standard" despite failing to carry out penetration testing on its website.
- Boomerang received approximately 1,100 complaints and enquiries as a result of the security breach.

Amount of fine

The Commissioner decided that the appropriate amount of the penalty was £60,000 to be paid by 12 July 2017 (subject to a 20% reduction early payment).

Comment

Although it won't be of much comfort to the Berkshire-based business, Boomerang got off reasonably lightly since the ICO has the power to impose a monetary penalty on a data controller of up to £500,000. TalkTalk was fined £400,000 by the ICO for failing to guard against a similar attack. In relative terms, however, Boomerang has taken a much bigger hit than the telecoms PLC. The danger now is that the ICO will become increasingly fed up with businesses failing to safeguard against well-known software vulnerabilities that have well-publicised fixes, such that fines will increase – a sobering thought in light of the imminent hike in penalty thresholds under the GDPR. Ominously, in alluding to the GDPR, the ICO has used this latest sanction to sound a warning to data controllers that, regardless of size, failure "*to take basic steps to protect customers' information from cyber attackers*" could have serious financial repercussions.

A particularly irksome feature of the case for the ICO would have been the fact that the overlook on the part of Boomerang occurred for no good reason. This laissez-faire attitude is unacceptable – anyone who processes personal information must comply with the eight data protection principles. As Boomerang found to its cost, failure to comply with the security requirements of principle 7 can come back to hit you hard.