Client Alert: Managing third party ransomware risk: Blackbaud

Date : July 28, 2020

Introduction

Ransomware raised its ugly head again in the news last week when a number of educational institutions and charities in the UK announced that they had been affected by the Blackbaud ransomware attack. The case illustrates some of the difficulties involved when those you do business with are compromised.

Ransomware is on the rise and as we said in our alert in March (see https://bit.ly/cvransom) there are special risks at the moment which criminals are seeking to exploit. Our alert in March explained some of the different types of attacks we are seeing. Some technical terms are used in this note which are explained at www.bit.ly/gdprwords.

What happened?

Blackbaud is one of the world's largest providers of CRM systems for the higher education, healthcare and not for profit sectors. In recent years it has acquired a number of different organisations including the funding platform JustGiving. It describes itself as "*the world's leading cloud software company powering social good*."

According to Blackbaud, it discovered in May 2020 that it had had a ransomware attack on its systems. It said that some data was compromised and a number of universities and other organisations using its services had been affected. Apparently Blackbaud waited until 16 July 2020 to tell its customers.

Despite the fact that the notification was well outside GDPR's 72 hour notification period, it seems that details are still scarce. Blackbaud has confirmed that it paid a ransom to the criminals involved.

Organisations who say they have been affected by the breach include:

- Aberystwyth University
- American Civil Liberties Union (ACLU)
- Bristol University
- Crisis
- De Montfort University
- Human Rights Watch
- King's College London
- Loughborough University
- Oxford Brookes University
- Selwyn College, Cambridge
- Sheffield Hallam University
- The National Trust
- University College, Oxford
- University of Birmingham
- University of Exeter
- University of Leeds
- University of Newcastle
- University of Reading
- University of Strathclyde
- University of Sussex
- University of York
- Young Minds

Blackbaud's website was still experiencing issues when we visited on 28 July. Blackbaud also has connections with a number of other major charities including Greenpeace.

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

Are Data Processors obliged to report data breaches?

Yes. Whilst the main obligation to report a data breach to the relevant Data Protection Authority under GDPR (without undue delay and, where feasible, not later than 72 hours after having become aware of it), under GDPR Art.33(1) is on the Data Controller, the Data Processor also has an obligation to notify a Data Controller without undue delay after it becomes aware of a data breach. This obligation was recently emphasised by the Swedish DPA in the NGSC case. We wrote about that case here www.bit.ly/swedegdpr. Data Controllers using Blackbaud will want to ask it why the report was delayed.

In this case we understand that the UK's Data Protection Authority, the Information Commissioner's Office (ICO) has been informed but we are not yet sure who told them. Regardless of who notified the breach, the ICO has the power to ask Blackbaud for more information relating to the breach. Under GDPR Art. 31 Blackbaud, like all data processors, has a duty to co-operate. GDPR Art. 58 also gives a DPA various powers to investigate including the right to carry out an audit of a data processor or to access any premises of the data processor and any data processing equipment on those premises.

What data was taken?

Again this does not seem entirely clear. At least one Data Controller has said that it is relying on assurances received from Blackbaud that the stolen data did not include bank account or credit card details and that the data was destroyed and not shared with third parties. The organisation concerned seems to be relying however, ultimately, on statements made by the criminal and it should be questioned whether in the circumstances anyone should be relying on the word of somebody who has already broken the law.

Will there be litigation?

Probably? At least one law firm has already said it had been instructed by individuals allegedly affected by the breach and it has started advertising for more people to join a possible group action. Group actions like this are not as attractive after the Morrisons ruling in the Supreme Court in April (see here https://www.corderycompliance.com/uk-court-of-appeal-ruling-in-morrisons-vicarious-liability-case/) but that is unlikely to stop proceedings being issued. In most cases it is likely that individuals will seek compensation from the Data Controller they dealt with (such as a university or charity) but GDPR does allow for litigation against a Data Processor (under GDPR Art. 82) and there's a mechanism in GDPR for attributing the damages between the Data Controller and Data Processor which will work alongside any contractual provisions. From our experience of handling similar breaches Data Controllers who have been affected by the breach would be wise to prepare for claims and for increased subject access requests.

What can organisations do to avoid this happening to them?

As we said in our alert in March (here www.bit.ly/cvransom) ransomware is on the rise and criminals are increasing the number and sophistication of attacks, particularly during the current pandemic. Organisations need to strengthen their defences and that will include doing proper due diligence on the Data Processors they use. Due diligence is obviously even more important given the recent ruling in the so called Schrems III case on data transfer (see www.bit.ly/pshielddead).

As part of the due diligence exercise you should make sure that the provider has adequate technical and organisational measures in place. You could draw up a checklist of your requirements perhaps based on the 14 steps that we suggested in our alert in March.

Organisations will also want to want to look in detail at their contracts with vendors and other third parties. They will need to look carefully at emphasising a Data Processor's obligations to let them know immediately if they suspect a possible breach. In our view audit rights on suspicion of a breach are also important – too often Data Controllers are vague about cause and effect and it can take the exercise of audit rights to get proper information. The contract should also back the Data Processor's obligations with proper penalties when things go wrong. All too often we see Data Controllers agreeing to contracts which cap liability at unrealistically low levels. That is unlikely to be a

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

defensible position under GDPR.

Consider a contractual obligation not to pay ransoms

All too often, once a ransom is paid, some gangs share details of who has paid on so called "*suckers*" lists. Paying a ransom once is no guarantee that you will never have to pay again and Data Controllers might at least want to be involved in any discussion or have the right of veto over ransoms being paid which affect data of which they are the Data Controller. Arguably, paying without the Data Controller's consent may breach other clauses in an agreement – but it would be wise to make your position clear.

It is important to remember that paying a ransom could lead to additional legal liability too. For example some organisations demanding a ransom could be on sanctions lists. In some circumstances making a payment could also contravene anti-bribery legislation.

Insurance

We are hearing at least anecdotal evidence that some ransoms are being paid by insurers to reduce their risk. If you have cyber liability insurance you might want to look carefully at your insurance contract to make sure that it does not give the insurer a right to pay ransoms against your will.

Conclusion

As we said in March, ransomware is on the increase and its effects are likely to be increasingly severe as organisations rely more on third parties to provide essential services. In most cases it is a myth that a ransomware attack need not be reported to a DPA. We are likely to see DPAs become more and more involved in the investigation of ransomware attacks and organisations must do all that they can to be prepared.

These are challenging times and organisations will have to balance multiple priorities currently. The threat is real however and organisations should do what they can to become more resilient given the rise in attacks.

For more information on how we handle data breaches see here https://www.corderycompliance.com/dealing-with-a-breach/.

Blackbaud's statement on the attack is here https://www.blackbaud.com/securityincident

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.