IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

IT Security

So, What's Our Response to a Data Breach?

Luke Brown

Luke Brown
Vice President – EMEA
WinMagic

Biography

Luke Brown is Vice President for EMEA at WinMagic (www.winmagic.com) and is responsible for managing the company's growth in EMEA. He has over 20 years' experience of building highly successful sales and customer support operations, in both new and mature markets, and has held senior leadership roles at both start-ups and listed technology companies.

Based in Mississauga, Ontario, WinMagic provides key management for all encryption needs. With the leading SecureDoc product line, WinMagic continues to provide easy-to-use and robust data security solutions for wherever data is stored, providing enterprise grade encryption and key management policies for all operating systems.

Keywords Data breach, Compliance, Corporate responsibility, GDPR, Encryption, IT Security, Reputational risk
Paper type Research

Abstract

A data breach is a serious incident for any business. The reality of a data breach is that it's not if, but when will it happen to your company. In this article, the author explains why the question "so, what's our response to a data breach?" should never be greeted with blank expressions in the boardroom.

Introduction

A data breach is a serious incident for any business. Often boardrooms make the mistake of thinking that a breach only relates to situations where a hacker has extracted information. For instance, the Uber breach in which 57 million names, email addresses and phone numbers had been exposed, or the now infamous TalkTalk breaches, which resulted in substantial fines and the loss of customer trust. But the truth is any data accidentally sent to a third party, or lost on a device, could constitute a data breach, not just the hacks.

Every board member should know the company response to a data breach if it happened to them, however most are more likely to think "So, what's our response to a data breach?"

The reality of a data breach is that it's not if, but when will it happen to your company. A corporate wide approach needs to be taken to developing a breach plan covering legal responsibilities, customer service, supplier relations, IT, marketing and communications.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

If you do not know how your company would respond, then the alarm bells should be ringing loudly. Data breaches are a boardroom issue, with almost every department affected in some way when one occurs.

Wherever data is stored it needs to be protected, particularly if it is sensitive corporate data or customer information covered by legislation, such as the incoming EU General Data Protection Regulation (GDPR). This legislation will see companies required to carefully manage the encryption, storage, use and sharing of that any personally identifiable information. Failure to comply can result in fines equivalent to 4% of annual turnover or €20 million, whichever is the greater, from 25 May 2018.

EU GDPR reinforces the utmost care that must be taken with data. The simple fact is that businesses must get the controls in place to manage their data, including taking the strategic decision that anything they would not want to see in the public domain, must be encrypted.

I will say it again – it doesn't matter where data is stored, it is still your corporate responsibility. A recent WinMagic survey[1] of 1,029 IT decision makers, found that 98% use cloud services as part of their IT infrastructure, with an average half of the infrastructure delivered in this way. That is a great example of how companies are embracing new technology, however, 61% felt they were not ultimately responsible for the compliance of that data.

Worryingly in the same survey a third (33%) admitted to data only being partially encrypted in the cloud, and 39% lacked a complete security audit trails across their infrastructure, leaving them exposed.

One of the key GDPR components is ensuring personally identifiable information (PII) is both anonymized and adequately encrypted. Encryption in particular is an approach companies can employ with all sensitive data, not just PII, to protect themselves against data breaches. Encrypted data if lost or passed to unauthorized hands, remains illegible and useless. This will greatly minimize the impact of a data breach on your business and is the last line of defence when all other security measures fail.

Don't bury your head in the boardroom

If any of the points raised here have placed a question mark over the security of your data and preparedness for dealing with a data breach, then the time to act is now. On 25 May 2018, EU GDPR comes into force and the weight of the law and subsequent penalties for non-compliance grow dramatically. Remember, every day there is the potential for a data breach, accidental or otherwise – you need to be ready to act at a moment's notice.

Reference	
1	For more information on the survey see www.winmagic.com