Do you value your security?

Security is the cheaper option – stop avoiding it

Taz Wake
Halkyn Consulting,
Security and Risk Management Specialists

Introduction

It seems 2012 was the year of Data Protection Act (DPA) breaches, and associated publicity and punishment from the Information Commissioner's Office (ICO). At the time of writing (Feb 2013) it seems this pace of breach has slowed down, but as the European Commission is looking to extend mandatory reporting requirements[1], it may only be a matter of time before bigger fines start to appear.

What is consistent is that in almost every published breach, from the high profile hack of Sony to quietly lost USB disks, the security breach has been a result of a management failure in how resources are allocated to security.

This short term-budget view consistently has a long-term harmful effect on organisations.

All too often, budget holders see security as a cost to the business and are then rewarded corporately for reducing the expenditure (not just through direct budget reductions, this is also done through badly thought out outsourcing, and excessive use of largely irrelevant technology). Unfortunately for the organisation, eventually this cost saving will cause a problem and, historically, this costs significantly more than the initial security spend would have been.

Case Study – Data Protection Act Fines

For this study, we will look at the DPA fine (civil monetary penalty) announced on 25 Oct 12, which was largely the result of risk management mistakes, meaning that a cheap preventative measure was ignored and, instead, a fairly hefty fine was paid.

The fine came as a result of a solicitor acting on behalf of Stoke-on-Trent City Council sending out emails containing sensitive data over an insecure channel. From the ICO's announcement[2]:

> ***If this data had been encrypted then the information would have stayed secure. Instead, the authority has received a significant penalty for failing to adopt what is a simple and widely used security measure.***

This is a pretty damning statement.

[1] http://www.halkynconsulting.co.uk/a/2013/02/mandatory-reporting-of-data-security-breaches/

[2] http://www.ico.gov.uk/news/latest_news/2012/penalty-highlights-need-for-encryption-of-sensitive-data-25102012.aspx

In most organisations, the first approach would be to identify the person who had compromised the data and investigate them with a view to disciplinary action to pass-off the ICO fine. However in this instance that doesn't seem to have been an option:

> ***The ICO's investigation found the solicitor was in breach of the council's own guidance which confirmed that sensitive data should be sent over a secure network or encrypted. However, the council had failed to provide the legal department with encryption software and knew that the team had to send emails to unsecure networks. The council also provided no relevant training.***

So the Council has gone to the effort of producing guidance on what should be done but **failed** to deliver the proper training and **failed** to provide suitable tools for the task.

If the Council had invested £10,000 in security training and a further £10,000 in implementing a good encryption package, they would have been able to save £120,000 in fines – a six fold return of investment. The reality is that the upfront costs would have been significantly less than £20,000 as WinZip would have been a perfectly suitable choice of encryption tool here and 500 only licences cost £2195….). Unfortunately for the Council, all they have done is delay the costs of providing the training and implementing the tools – they will have to pay that as well as the ICO fine now.

This breach, and £120,000 fine is very similar to one recently imposed on Greater Manchester Police, who were fined the same sum of money on 16 October 2012[3], following the burglary at the home of an officer which resulted in an unencrypted USB stick being stolen. Use of the free and open source software TrueCrypt would have saved them from the fine (*even assuming they had to pay £10,000 to train staff in its use, they would have avoided £110,000 worth of penalty*).

Outside the UK, the matter gets worse where there has to be greater consideration of the number of records breached. In an example based on Gartner's findings[4], it has been reported that a data breach can cost 70 times the cost of implementing encryption.

Whatever the jurisdiction, with or without a regulatory obligation, the fact remains: **this boils down to a risk management choice**.

[3] http://www.ico.gov.uk/news/latest_news/2012/police-force-pays-120000-penalty-for-data-breach-16102012.aspx

[4] Reported at http://www.fiercemobileit.com/story/laptop-data-breach-can-cost-70-times-more-firm-wide-encryption/2012-10-25

You can opt to implement the correct measures from the outset, accept that you will be paying something but it will be less than the costs that will come from a breach (fines, loss of customer confidence, brand damage etc.) or you can opt to take the risk.

If you have made the decision to take the risk, you absolutely must make sure you put aside sufficient funds to cover the damage you are likely to face and the costs of remediating the issues you have chosen to avoid. There is no free lunch here.

Anything other than these two choices is not risk management, it is just closing your eyes and hoping nothing goes wrong. Barely a week goes by without there being evidence that this is a forlorn hope.

So, take this opportunity to learn from the lessons here, review your processes, training and tools and make sure you have adopted a proper risk managed approach to the risk of a data breach. At least that way, if you have a breach, you are properly positioned to deal with the consequences.

About Halkyn Consulting

Halkyn Consulting Ltd is a specialist security consultancy based in North Wales, experienced in providing security advice to local, national and international clients including government agencies, multinational corporations, small businesses and homeowners.

For more advice on how to properly use passwords or any other questions you may have related to security and protecting your home, business or other assets, you can reach Halkyn Consulting on the web at www.halkynconsulting.co.uk by email to info@halkynconsulting.co.uk or you can call us on +44 1522 940 858.