White Paper: Data Security

Data Breaches: Expectation and Reality

Sharon Frost
Faronics UK
+44 (0) 1344 741057
sfrost@faronics.com

Introduction

In November 2012, The Ponemon Institute released the *State of Cyber Security Readiness: UK Study* report, under the sponsorship of Faronics. The aim of the study was to determine how prepared small to medium UK businesses were for the very real threat of cyber attack, and in the event of such an attack, what the consequences would be for the businesses in question.

The study, which took in individuals from 544 different small-to-medium businesses, highlighted a number of issues regarding data security preparedness, including the somewhat startling fact that a 54% majority of those questioned had experienced security breaches within the past 12 months. However, the major cause for concern wasn't to do with the proliferation of data breaches across UK SMBs, but was instead linked to the misconceptions surrounding data breaches shared by those yet to experience such a problem.

The threat of data security breaches

Data security breaches can occur in any number of ways. If you were to ask the majority of the general public where they expected a data breach would be most likely to originate, they'd tell you that malware attacks and online data theft were the greatest threats to corporate data security. While data theft is a genuine problem that many small-to-medium businesses will have to defend themselves against in time, we have found that the majority of corporate data breaches are the result of mistakes or malpractice on behalf of the end user. 55% of those questioned identified 'employee mistakes, incompetence or negligence' as the greatest contributing factor to digital security breaches, while 32% also selected a 'lack of guidance from management' as a major problem in the preparation against data security threats, suggesting the issue runs deeper than the odd employee mistake.

While the threat of a data security breach is very real and very serious, the misinformation regarding data security is a stumbling block over which a surprising number of businesses are destined to trip. If you thought that a data breach would only cost you time, money and potentially valuable information, you're sadly mistaken. Of all respondents who had been recent victims of data security breaches, a staggering 48% said that the very reputation of their company had been damaged as a result of he incident.

As was revealed by the Ponemon study, a great deal of frustration is generated as a result of employee mistakes and misdemeanours regarding digital security. This feeling of frustration is further borne out by the statistics, with as many as 30% of respondents saying that they were forced to lay off employees as a result of a data security breach. It's obvious that the potential risk and costs of a data security breach are manifold, and sadly, few businesses are in a position to expect them.

Data breaches and corporate naivety

During the Ponemon study, we spoke to numerous UK SMBs and compared their experiences of data breaches to their expectations of risk before the event. When asked about the potential damage to corporate reputation and brand image, one individual who preferred to remain anonymous remarked:

"It had never really occurred to us that a data breach could affect the reputation of our brand. I suppose if we ever though about it we just assumed that anything like that could be kept under wraps or dealt with internally. Then, when we did become a victim of a security breach, we found that our customers were more reluctant to trust us with their data than they were before.

In truth, it hurt us badly.''

Their statement mirrored the experiences of many respondents questioned in the course of the *State of Cyber Security Readiness: UK Study.* As we've already mentioned, almost half of the companies who had fallen victim to data breaches in the past found that their reputations were damaged as a result, but this statistic sits in stark contrast to the number of companies who expected such a result in the first place. Only 39% of respondents who were yet to suffer a data breach expected such a security failure to fall back on the reputation of their brand, let alone as radically as detailed in the case study above.

It's a similar story when you look at the involvement of staff and employees in previously documented data security breaches. As we mentioned before, few people would expect a digital security threat to originate from mistakes within their own company, at least not to such a degree that peoples' jobs would be at risk. Predictably, many of those questioned were sceptical when asked whether they would expect to lose staff members as the result of a data breach, with a paltry 7% of those who had not been involved in a breach expecting the axe to fall in the aftermath of an internal security blunder. Contrast this with the 30% of affected companies who had to let staff members go in reality, and you can see that a culture of misinformation has risen around the idea of data security breaches, their risks and causes.

Risks of unpreparedness

The risks of data breaches can come from numerous sources, some of which you may not have expected, and may have numerous consequences, few of which the average business will have been prepared for. But what could a lack of adequate preparation for data security breaches, as evinced by our sample, end up meaning for your business?

- **Reduced clientele** – If a data breach were to affect your company's reputation as it did for 48% of our sample, your business would more than likely find it increasingly difficult to build on your existing client base, win more custom or expand.
- **Minimised trust** – Business / client relationships are very delicate things, and any small shift in the dynamic can have a negative effect on the way in which your customers view your business. If you've been the victim of a data breach, your customers may be less likely to trust you with their accounts and personal information in future.
- **Loss of funds / trade secrets** – Evidently, there's more to many data breaches than the knock-on effects to your business. The data you lose may contain bank account details, trade secrets or other desirable pieces of information that you wouldn't want to fall into the wrong hands. The damage this could do to your business needs no explanation.

- **Turnover of staff** – If a data breach has come as a result of mistakes, incompetence or negligence on behalf of your employees, you may have to let some of your staff members go, as 30% of our security-breached respondents found to their cost.

One of our respondents, who preferred to remain nameless rather than bring their company into further disrepute, found that the costs of data breaches extend far further than most people realise.

"Of course, we strove to be as compliant as possible when it came to digital security, but you can't always account for the behaviour of all your employees. Our breach came via the inappropriate use of a company laptop, and we lost a great number of important documents as a result. As if that wasn't enough, we had to move the employee in question on and fill the vacated position, which only ended up costing us more time and money."

Unless your company is sufficiently prepared for and protected against the threat of digital security breaches, you could find that the cost of one insignificant mistake could spiral up and up.

Mitigating the risks of data breaches

Information such as that provided by the Ponemon study is invaluable in helping to prepare your business and its staff for the threat of data security breaches. Just knowing about the hidden risks, misconceptions and out-dated practices involved in data security can help to mitigate the risks of a data security breach, but there are other steps your company can take to ensure that you're less likely to become a victim yourself.

Internal compliance policies

Are your internal compliance policies up-to-date? The rate of technological growth and development is such that new risks and problems can occur almost without your knowledge – even a two year old compliance policy may be ludicrously out-dated by now. The Ponemon study found that respondents identified end user devices like BYODs (Bring Your Own Devices) as representing the most significant data security threat to their businesses, and these days it is by no means uncommon for workers to use their own desktops, laptops, smartphones and tablets to work on the go or at home. Do you have compliance procedures and protocols in place to cover these devices? If not, now should be the time to do so.

Communication

Alongside the risks represented by the negligence, mistakes or incompetence of staff, our respondents identified a lack of adequate communication and instruction from managers and supervisors as a major source of data security frustration. Lines of communication between employees and managers need to be open and clear – it's no good expecting certain standards from your staff if they don't yet know what those standards are. Your employees need to know what's expected from them in terms of data security and online safe practice, so take the time to tell them what they should be doing to ensure that your company's data does not come under threat. Let staff know what your digital security software is for, how it works and what its strengths and weaknesses are. If all of the relevant information has been shared between staff and managers, there really should be no excuse for a digital security breach.

Data breaches and digital security

While you can always take steps to ensure that your staff and managers are as compliant and as aware of the risks of data security breaches as possible, there can still be no accounting for human error. The human element of your company will inevitably make mistakes every once in a while, while there will be those who feel that company compliance policies does not apply to them, or that data breaches aren't as much of a threat as they're made out to be. Updating your company's compliance policies or concentrating on training your staff and managers will only be able to do so much when it comes to the outright prevention of data breaches, so your company will need to think long and hard about your current IT security solutions.

The Ponemon study revealed that a staggering 67% of respondents spend less than 10% of their total IT budget on digital security solutions, and yet it is these solutions that can have the biggest impact on reducing data security breaches within your company. The greatest benefit of investing in data security solutions was found to be a decrease in the frequency of data breaches, with 63% of respondents stating that the implementation of data security software corresponded with a drop in the number of data breaches, while a further 53% found that the software also increased machine availability and ultimately employee productivity.

Your company should be looking to implement a digital security system that not only offers protection for your data against malware attacks, but also reduces the workload of your IT department. When Augusta County started using Faronics' Core program in public schools, it found that tech support requests were reduced by more than 60%, as the majority of the IT department's time had previously been spent ridding systems of malware attacks and data security threats.

Faronics Core allows users to control a whole host of Faronics digital security software solutions from a single computer, and can help IT technicians to manage third-party software remotely, too. Instead of worrying about whether or not employees are following internal compliance protocols whilst using their work machines, Faronics Core allows the IT department to ensure that they're doing so at all times. As Faronics core is integrated with all of Faronics' other security software packages, too, it means that companies can shut out malware using the antivirus program and prevent unwanted third-party programs from opening by blacklisting them with Faronics' Anti-Executable. This way, even the least security-conscious employee shouldn't be able to open your data up to unwanted security threats.

The risks of data breaches are great and broadly misunderstood, but adequate preparation in the form of improved internal compliance protocols, open channels of staff communication and of course, top level digital security software can ensure that you don't get caught in the mire of data security misinformation in future. Forewarned is indeed forearmed.

About Faronics

With a well-established record of helping businesses manage, simplify, and secure their IT infrastructure, Faronics makes it possible to do more with less by maximising the value of existing technology. Faronics is the ONLY endpoint security software vendor to offer a comprehensive layered security solution consisting of anti-virus, application whitelisting, and instant system restore protection. Incorporated in 1996, Faronics has offices in the USA, Canada and the UK, as well as a global network of channel partners. Our solutions are deployed in over 150 countries worldwide, and we are helping more than 30,000 organisations.

Sharon Frost
Faronics UK
Venture House, 2 Arlington Square,
Downshire Way
Bracknell, RG12 1WA, England
Call Local: +44 (0) 1344 741057
www.faronics.com