White Paper: Small business data security

Could a data breach cause your business to fail?

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

Introduction

In today's digital world, most small businesses simply could not survive without basic computer systems, and still more would be lost without the internet. The data businesses collect is essential to profile and understand consumers, manage accounts and provide the most effective services and products in a crowded and competitive market.

However, lurking beneath this essential need is a hidden danger, which many small business owners are largely unaware of. A recent UK survey sponsored by Faronics studied how UK businesses viewed data security, seeking to understand exactly what precautions were being taken and what the results of specific data breaches have been. 544 individuals from organisations with a headcount between 50 and 3000 were surveyed; 54% of these had experienced a data breach in the past 12 months.

This White Paper profiles two small businesses that we studied alongside the wider survey; their habits and the consequences of their data breaches reflect a number of similar stories told by other small businesses uncovered in our survey's research. The eventual failing of both businesses less than a year after the breach should act as a shocking indication of the risks that many small businesses face, and what steps other businesses should take to prevent the same actions and patterns from being repeated in their own firms.

The Shape of a Data Breach

Whilst a data breach can take many different forms, the two small businesses we have chosen to profile in this instance are typical in that they reflect the unexpected nature of a data breach, the different entry forms it may take, and its wider spread to other areas of a small business. The first organisation, a payroll agency that had hundreds of clients, was dissolved in the space of a year as a result of a data leak; the second manufacturing organisation stopped trading within 8 months after its breach took the form of corporate espionage. Though shocking, these are accurate representations of the rapid and devastating effects of inadequate security protocols, despite both firms working to implemented data security compliance guidelines.

Data Security

Naturally, most client-orientated companies working with sensitive data will have taken some steps towards its wider protection. Whilst many will do this primarily out of a sense of responsibility and a need to meet compliance regulations, it is evident that an incomplete approach is being taken in this process. The payroll firm we spoke to described how they closely followed the regulated guidelines for data protection, yet were still the victims of a data breach that devastated their business entirely.

In this instance, a laptop taken home from work was infected with a piece of malware, which then spread across the professional network. The breach was limited to the attempted hack on the firm's own bank account and an estimated leak of around 1% of client account details. Despite the tiny scale of this, clients had to be informed, and the firm saw their hard-earned trust melt away. Whilst they had previously been considered a dependable and secure organisation, the data breach meant that most of their clients simply could not afford to take the risk.

Faced with a sizeable loss of income and the decimation of most of their existing client base, there was no choice but to make a number of their staff members redundant and concentrate their financial savings on acquiring new clients and customers. Details of the data breach then made it into the press, and it soon became evident that their expected 6 month long recovery process was simply not an achievable aim. When the first results of a Google search of their name was not their own website, but instead a number of press articles relating to the breach, it became clear that all public credibility had been destroyed. After just under a year of attempting to recover from the data breach, the directors made the difficult decision to dissolve the firm. The cost of the data breach is estimated to have been well into the hundreds of thousands.

Corporate Espionage

For a manufacturing company established by two bright Oxford engineering graduates, there seemed little reason to implement complicated data protection procedures. Using knowledge gained through their time at University, the duo had developed a series of manufacturing processes and machines that boasted extremely high energy efficiency, allowing them to create high quality plastic products at a lower cost than the market average. With this as their starting point, they soon went on to develop other products, and the company steadily expanded.

In early 2012, however, they were the victims of a data breach thought to have originated from a rogue online application run by one of their staff members. Despite having anti-virus software in place, which they had felt would be enough, the results were devastating. “We didn’t think we had anything unique worth protecting within our business,” one founder confesses. “It almost felt as though because we worked with our processes day-in, day-out, we weren’t doing anything drastically different to our competitors.”

The first evidence of the data breach surfaced when many of their existing contracts left to other businesses, who for the first time could offer the same quality at a lower cost. After some research, it was found that a series of revealing manufacturing guidelines were available online, literally giving competitors a step-by-step guide to production. Antivirus software had done nothing to protect the firm from a Trojan that scraped this vital information from their systems.

Within a matter of weeks, their manufacturing procedures had been adopted by a number of larger manufacturing companies that had the scale to offer more competitive prices to their consumers. With neither suppliers nor consumers, their sales efforts were in vain. As the incriminating information was available widely online, the problem of data protection became too widespread. No route could be traced back to the likely perpetrators; no legal action could be taken. Within eight months, the company could no longer compete with the larger market. Their niche offering and differentiation from the larger players had been removed, and they soon folded.

Data Breaches: Unexpected Wider Impacts

In essence, data breaches have both immediate and wider-reaching effects on a small business, both of which were seen in the examples outlined above. Our research suggests that businesses were faced with average costs of £138,700 and a 9.3 month recovery period; this jars substantially with the underestimates put forward by organisations who had not suffered a breach, estimating a maximum cost in the region of £95,000 and the recovery period to normal would be around four months.

With these results, it is evident that many small businesses cannot be fully aware of the effects, both short and long term, that a data breach is likely to have. The short term effects, often viewed as the most devastating, are likely to include a number of the following:

- Loss of finances through account hacking, compensation payments or imposed fines.
- Cancellation of existing client, consumer and supplier contracts, and broad impacts upon customer loyalty.
- In the event of data loss, costly and time consuming repetition of work that has already been completed.
- Obligatory redundancy of staff members and downsizing to recuperate loss of company finances and on-going contracts.
- Costs of outside consultants and lawyers to recover from the breach.

However, what many businesses must be failing to consider in their estimations of the cost of a data breach and the time it takes to recover are the longer term effects a data breach can have on a small business that could lead to devastating results. These include:

- The devastation of public credibility
- Increased costs of customer acquisition, which our survey suggested could rise by an average of £91,985 after a breach
- Loss of advantage over the competition
- Increased difficulties in hiring staff members
- Difficulties in the further prevention of data breaches, as nearly a fifth of all respondents had experienced more than four.

Compliance is not enough

What is more than evident as a result of this survey is that firms cannot be doing enough to prevent data breaches, and as a result security failures are becoming alarmingly commonplace. Whilst compliance with data security regulations can often be achieved through the use of simple anti-virus software, it is clear that this is not enough to prevent a data breach that could lead to the devastation of many businesses, particularly smaller organisations without large reserves and safety nets. Common areas that are the source of worry for security teams surveyed include:

- Bring your own devices, which many small businesses are reliant upon. Only 38% of laptops and a shocking 12% of other devices in our survey had anti-virus/anti-malware protections
- Lack of security protection across all devices (73% of respondents admitted file and full disk encryption technologies were either not present or only partially deployed)
- Insecure third party software or cloud providers
- Proliferation of unstructured data with unclear storage locations
- Increases in the frequency and sophistication of malware and other viruses

Strategies to Prevent Devastating Breaches

Our survey suggested that despite the lack of uptake of various software protocols and practices, firms seeking to prevent data breaches seem to have the necessary knowledge. Over half of those asked suggested identifying and restricting access to sensitive information, protecting systems and establishing up-to-date internal policies to educate staff members about best practices. Despite this, all evidence points to a difficulty for firms in turning this knowledge into an actionable plan. The evidence suggests that this is largely due to the lack of in-house expertise to become cyber-ready. Over 75% of our survey's respondents admit to having insufficient people resources, with 55% believing that they require specialist personnel in order to understand complex compliance and regulatory requirements.

For Faronics, the survey has driven home the absolute necessity for organisations of a security product that offers a solution over and above what compliance procedures require as standard. In this manner, firms can then be sure that they are doing all that they can to protect their own and their clients' data. In addition to this, improved data protection systems would allow IT personnel to spend less time fixing failing systems, thereby resulting in increased uptimes of systems.

One such solution to this necessity is the provision of a layered security software approach similar to that which we provide. In this manner, anti-virus software is the first layer of protection, offering the broadest protection against attacks from well-established and known viruses, malware and spyware. Beyond this first layer, an anti-executable that either permits only whitelisted programmes to operate, or prevents blacklisted programmes from starting up, can then protect a system from well-disguised malware or Trojans that have not been captured by the anti-virus software. Faronics favours the whitelist approach, as this gives much greater control over unknown threats. Whilst the anti-virus and anti-executable software working in unison will protect most systems from most attacks, our approach also allows organisations to go one step further through the provision of Deep Freeze, which restores computers back to their original configurations with every restart.

With the implementation of control and profiling systems often viewed as a time and resource-intensive task, Faronics also provides solutions to make the tasks of IT departments much simpler. Faronics Core has been known to reduce the number of tech support requests by more than 60%, and through the use of WINselect and System profiler, small businesses will be able to carry out IT maintenance tasks quickly and simply, without great expense or required extra resources.

Summary

Data breaches present a real risk to small businesses. Despite a large number of firms having the knowledge of what best practices should be implemented to prevent a data breach within their organisation, a lack of time, human resources, priorities and awareness of risk have meant that over half of those surveyed have already faced what could become a fatal error. If small businesses are to address the issues at hand, they must work to employ preventative measures that go over and above those in line with required compliance, particularly when working with new technologies and systems. Without preventative actions, it is clear that many will incur costs of hundreds of thousands of pounds, which could well spell disaster for those at a critical period of their growth.

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