SECURING THE FUTURE

In this Issue

The many costs of a data breach

In this issue, we will examine the various ways an organisation may be negatively impacted if it were to suffer a data breach.

The 2013 Shred-it *Information Security Tracker*, conducted via Ipsos Reid, revealed that only 40 percent of small business owners and 70 percent of large business owners are aware that a data breach could result in severe financial impact and harm the credibility of the business[1]. These statistics reveal that the vast majority of UK businesses, both large and small, are generally unaware of the many costs that may be associated with a data breach. Most seemingly believe that a data breach is a one-time affair with few – if any – long-term consequences.

In reality, data breaches can have numerous long-term negative impacts, many of which might be unexpected. For example, organisations may experience a loss of revenue, loss of reputation, have their business opportunities dwindle and, most importantly, they may lose the trust of employees, customers and shareholders. With this in mind, this newsletter will provide you with insight on the various costs of a data breach and provide helpful tips to avoid becoming a victim.

1 2013 Security Tracker "Perceived impact of lost or stolen data on business"

SECURING THE FUTURE

The bell never tolls just once:

The next time an organisation thinks a data breach can be easily contained and its impact minimised, consider this story:

> *Last month, one of your company's rising stars was on the road signing a major deal with a new distributor. On their way back to the office, they accidentally lost the financial information outlining the deal. They were unsure how this happened, but when you found out about the incident the following Monday you had to make the difficult phone call to your new distributor. The ink had barely dried when the partner backed out of the deal, citing an inability to trust you after having lost their financial information.*
>
> *Because of this breach, your company lost out on a deal that would have guaranteed business growth until the end of the fiscal year. But the costs don't stop there, and instead begin piling up for you and your associates. Thinking you might be able to salvage the situation, you reach out to other distributors, but all you find are dead ends. The story was leaked to the media and now you've lost your hard-earned reputation as few in the business community now trust you. Your quarterly estimates quickly fall and revenue drops. With a limited market and no potential, you begin shedding staff. On top of this, your company is embroiled in a legal battle stemming from the original breach.*

An *opportunity cost* is a reputation lost

The Ponemon Institute's *2013 Cost of a Data Breach Study* classifies the losses detailed in the above story as a form of *opportunity cost*. This can be defined as lost business opportunities resulting from negative reputation effects following a breach (and publicly revealed to the media)[2]. This study found "that the negative publicity associated with a data breach incident causes reputation effects that may result in abnormal turnover as well as a diminished rate for new customer acquisitions"[3]. In essence, most companies experienced opportunity costs associated with the breach incident, which diminished their ability to attract and retain new and existing customers.

2 Ponemon Institute's 2013 Cost of a Data Breach Study, page 22.
3 Ibid, page 20.

Back to the Top

SECURING THE FUTURE

Don't err, be aware!

With 35 percent of data breaches attributed to human error, organisations may want to reconsider their perception of the potential impact of a data breach[4]. In order to avoid this most unfortunate fate, organisations can take a number of steps to protect sensitive information:

- Implement ongoing risk analysis processes and create a policy specifically designed to limit exposure to fraud and data breaches
- For employees working on-the-go, ensure your information security policies and procedures include mobile security rules and precautions
- Train and review your information safety protocols and policies regularly with staff and ensure policies evolve alongside changes in your workplace
- Encourage employees to maintain full control over all vital information, inside and outside of the office
- Consider a shred-all policy for all documents that are no longer necessary
- Don't overlook electronic devices or hard drives on computers and photocopiers; physical hard drive destruction is proven to be the only 100 percent secure way to permanently destroy data from hard drives
- Remind employees that information security is even more important when outside the office

When it comes to protecting sensitive information, an organisation can never be too careful. By following the above tips and being aware of the impact of data breaches, organisations can arm themselves against the many potential long-term effects that result from a data breach.

Your Free Security Consultation

Shred-it has developed a survey to help businesses better understand security gaps. Download the factsheet and conduct your own security self-assessment.

Learn more about Shred-it services or book your FREE security assessment.

You can also stay informed with Shred-it on Facebook and LinkedIn or follow us on Twitter at @Shredit_UK.

4 Ibid, page 7.

Back to the Top