IBM Midsize Insider Blog

Title: How Much Do Data Breaches Cost?

What is the cybersecurity price tag worth? Two recent studies attempted to put a number to it. However, getting a good grasp of what is really at stake isn't so easy. When it comes to midsize firms, more is at risk.

Factoring the Loss

An article in Information Management highlighted how the American Bankers Association and Kaspersky Lab took a close look at cybersecurity losses recently. Kaspersky Lab revealed that lost financial data ranged from $66,000 to $938,000 per organization, depending how big the firm was. The cost of actual fraud losses, consultants and lawyers to help manage the breach as well as lost business opportunities were factored in. Meanwhile, the ABA took a look at loses after a major corporate breach and found that the loss on a fraudulently used debit card was $331. ABA also found that eight percent of debit cards were used for fraud while credit cards were used four percent of the time.

Overall, bank technologists must take a close look at the losses from security breaches that have happened in recent past to evaluate what was lost but calculating the entire loss isn't so simple because the effects go beyond the company. Individual reputations, careers, morale, stock value are all affected. Additionally, customer services and operations are also working longer hours to fix problems. Turns out, the biggest cost to a firm after financial fraud is the downfall on customer service.

Big and Small Breaches

While it's true that breaches at big corporations make headlines it's also true that midsize firms are just as much at risk to cybercrime. Smaller firms are often considered more appealing because they are considered "low-hanging fruit." Many cyber criminals rely on the idea that IT professionals at these firms don't have the expertise to truly secure their IT which means malicious deeds have a higher success rate. As a result a breach may go undetected for a long time. The affects can be devastating compared to what big name firms experience. With little resources to fight back and recover a breach can be hard to recover from or may even close down a smaller firm.

Midsize IT professionals that simply don't have the resources to keep up with the latest financial IT security solutions have a growing opportunity to work with trusted security vendors to fill the knowledge gap. By paying close attention to new solutions in the growth of third platform technologies like cloud and big data, as well as the move toward Internet of Things solutions, a

IBM Midsize Insider Blog

Title: How Much Do Data Breaches Cost?
growing firm can be ready for challenges that may come and at least prevent some breaches easily.

Far Reaching Effects

Recent studies show the cybersecurity price tag is hard to truly monotonize because the affects can be far reaching. It's a big problem that affects all firms and especially midsize business. Despite the attention given to major data breaches, smaller firms have a lot to lose – fast - but with the right counsel IT professionals can optimize their IT to be prepared. It is possible to deploy innovative solutions to thwart tomorrow's threats.

##

Published September 2014