# What's in a Name?

Michael Peters | April 25, 2011

Michael Peters, Vice President - Chief Information Security Officer, CrossView

Prior to April Fools' Day, 2011, you probably had never heard of Epsilon Data Management, right? I'd wager, however, that this email marketing firm has heard of you. In excess of 250 million email account names were pirated from the marketing services firm, vaulting this to what may be the largest breach of personal information in U.S. history.

Epsilon is the company behind the high-profile leak of data belonging to some of the best-known and most respected brands in the world, including Best Buy, Capital One, Citigroup, Disney, Home Depot, Target, TiVo, Verizon, Visa and Walgreens … just to name the tip of this iceberg. If you have ever interacted with any of these brands, chances are your name and personal information were among the data stolen.

You might be asking yourself, "Why would Epsilon have my personal information?'" Companies frequently trust other enterprises to perform services in support of their business – in the case of Epsilon, marketing services. Unfortunately, many companies do not take security seriously enough. In fact, a recent study conducted by the U.S Secret Service concluded that 79 percent of victims (read, companies) subject to Payment Card Industry Data Security Standard (aka PCI DSS) had not achieved compliance. The study also concluded that "48 percent of breaches were caused by insiders," which means employees and trusted business partners like Epsilon.

Prior to doing business with a company to whom sensitive data is released, the Chief Information Security Officer should always conduct a thorough examination of security controls and overall security posture – especially when client information is at risk. A company's reputation and customer well-being are paramount and that shouldn't be taken lightly.

If you are going to entrust sensitive data to a partner, you need to be asking questions like, "Do my service providers verify the security of their applications during installation or during my support cycles?" Have you considered that "Without security, my business is at stake and does my application provider take that seriously?"

As Chief Information Security Officer for CrossView, I can tell you unequivocally, that the commerce applications CrossView implements and supports undergo rigorous security certifications. You receive bona fide evidence to achieve PCI DSS compliance. You receive ongoing security support to maintain the highest level of security to protect your brand and your customers. We take security seriously – that's the secret.