Chapell & Associates, 236 W 10th St, Suite 23, New York, NY 10014 212 675 1270

Chapell & Associates

CONSUMERS STILL AREN'T CAREFUL ENOUGH WITH THEIR PERSONAL INFORMATION

Originally published in the DMNEWS *on January 23, 2006*

When Lewis Black told the *Daily Show*'s John Stewart recently, "If you think Americans are so smart, I know a Nigerian business man who'd like your email address," I wasn't sure what to make of it. Of course, the Daily Show is satire, and really – aren't consumers being more vigilant about their online privacy? There have been a number of recent reports detailing how consumers are spending less online, using fewer websites, and being more aware of pernicious technologies, all signs of increased caution.

But then again, satire is funny because it hits home. According to RSA, consumers are still far too willing to give out their personal information. The security company was recently able to acquire the mothers' maiden names of many NYC tourists by pretending to take surveys in central park. And don't forget that RSA and Verisign also found it quite easy, back in May 2005, to trade lattes for consumer passwords.

And yet I'm skeptical of the claim that consumers aren't doing enough: most reports that have come out in the last six months – those from PEW and Consumer Reports WebWatch, notably – would seem to contradict the RSA's claims. The PEW study has 48 % of online consumers avoiding some websites because of a fear of spyware, and WebWatch reported that 29% are shopping less because of privacy concerns. And Entrust has just found that nearly 20% of those consumers who bank online are now doing so less.

IS CONSUMER VIGILANCE ENOUGH?

But even if consumers are being more careful, we're still hearing about data breaches. Why is this? Well, many of the recent breaches occur through no fault of consumers. ChoicePoint recently informed another 17,000 consumers that their data had been compromised from its September 2004 data breach. And TransUnion LLC, a company that maintains consumer credit histories, just disclosed its own breach, with around 3,000 affected consumers (this is, unfortunately, a modest number, given the data breaches of the last year).

Most striking, in September security experts at major credit card companies told attendees of the Bank Card Conference that the struggle against online identity thieves had reached something of a stalemate. "They're a few steps ahead of us in a couple of areas," Joe Shaughnessy, senior vice president for fraud prevention at VISA USA said. "They've done their homework about the payments system and because of [them], we all have a chance to lose some sleep at night."

We seem to be hearing two things here. First, consumers still aren't careful enough with their personal information. But second, even if they were more careful, there still might not be a decline in identity theft. This is something of a contradiction, and it undermines the case for increased consumer vigilance. This has led some to argue that consumers can only do so much. Identity theft has often been thought about on an individual level – so-and-so has their identity stolen, here's what could have been done. But if personal information is stolen from businesses, and not from individuals, what's a consumer to do?

BUSINESS-SIDE APPROACH

A consumer can protect his or her own data only as long as they're holding onto it – once they entrust it a business it's literarily out of their hands. So while consumer education about online privacy is part of the equation, it can only go so far. The rest of the responsibility falls to those businesses that hold and use personal data.

The perception might be that protecting consumer privacy is just a technological issue – when personal information is stolen from a business, it's because someone broke into an insecure server, etc. But this isn't always true – when a few New York based colleges experienced their own data breaches recently, it wasn't because technology was misused or out of date. It was because someone accidentally put sensitive information up on a public website.

This is to say that avoiding data breaches and protecting consumer privacy isn't just a technology issue. So what can an organization do to avoid data breaches? It's not a simple answer, but there are three things any business can do to start with:

1) **Hire a privacy officer.** If your company stores or uses sensitive consumer information – be this social security numbers, addresses, or credit card information, having a fulltime privacy officer (or advisory committee) can be one of the most important things in avoiding a data breach. This way, someone is looking into the problem at all times.
2) **Engage all employees in privacy training –** or at least those who deal directly with consumer information. Data breaches can happen from the mistakes of one employee – it's important to have every person working with sensitive information understand how to safeguard and use it properly.
3) **Review what information is collected and how.** What information is collected from consumers? Does this include personally identifiable information (PII)? Who has access to the data? What third parties (if any) is this information transferred to?

These steps will help reduce the likelihood of a breach – but moreover, if a breach occurs, will give your organization some tools with which to respond. When once asked how he'd respond to a chaotic event, Jon Stewart said, "Most likely, I'm going to plunge my head into an ice bucket." If a data breach occurs, you might feel like pulling out the bucket of ice water. Fortunately, with some steps in place to overcome the effects of a breach, when you come up for air there'll still be time to breathe.

Alan Chapell, CIPP, is president of Chapell & Associates, a premier research and consulting firm focusing on privacy, marketing and permissions management. Mr. Chapell is a member of the DMA, the Mobile Marketing Association, the Direct Marketing Club of New York, and is the New York chapter co-chair of the International Association of Privacy Professionals. He publishes a daily blog on issues of consumer privacy, and can be reached at achapell@chapellassociates.com.