Data Breaches in 2010: How they happen and what your organization can do to prepare.

August 2010

The malware was so well-hidden that two separate teams of forensic investigators almost missed it.[1]

Before breaking down exactly how data breaches are happening, one fact needs to be addressed: they're happening on a bigger scale and affecting more consumers than ever. In 2008, records breached totaled 35,691,255. In 2009, that number jumped to 222,477,043 – resulting in 26% of consumers receiving data breach notifications and more than one in every four consumers replacing a debit or credit card due to security issues.[2] This growing problem affects company budgets as well as the backlash seen in consumer confidence and spending. So, where are the breaches occurring?

Data in Motion

This includes data moving into or out of a network via the Internet, email, webmail and file transfer protocol, among other avenues that move information. In the case of the Heartland Payment Systems breach, data sent across the Heartland network was copied and stored as .tmp files for third party retrieval. The malware was so well-hidden that two separate teams of forensic investigators almost missed it.[3]

Data at Rest

A decade ago, data at rest used to be the preferred target for hackers. Recently, there's been a significant shift to targeting data in motion. That said, data sitting in databases or file systems is still at risk and should be encrypted, with the keys used for encryption rotated at least once a year.

Data at the Endpoint

The least "techie" of breaches, endpoint data loss is largely due to human error. Lost or stolen laptops account for 21% of data lost. Furthermore, in a recent survey, the UK security company Credant found that 4,500 USB drives were left in clothing at the dry cleaners.[4] The more mobile we become, with smaller, more powerful technology, the more risk there is for leaving data in unsecure locations.

How Do Consumers React to All This?

Almost 40% of consumers who've been notified of a potential data breach use their credit or debit card less. While 38% hold banks responsible after receiving a data breach notification. A simple market sizing indicates that at least 72 million replacement cards were sent to consumers in 2009.[5] In short, consumers react predictably: they get their cards replaced, they lose confidence in their bank and they use their "breached" credit or debit card less.

Those are the immediate reactions of consumers, but there are other behaviors worth noting. These behaviors can help shape how your company responds to a data breach. For example, 28% of consumers who have been a victim of fraud purchase a credit monitoring service, a whopping 49% put fraud alerts on their credit report and 17% purchase identity theft insurance.[6] From this data, we can assume that credit monitoring service and identity theft protection would be a welcome follow-up to receiving a potential data breach notification letter. Customer retention post-data breach needs to be part of any organization's plan and can help mitigate the overall costs of a breach.

1-6 **Javelin Strategy & Research**
2010 Data Breach Prevention and Response: Causes, Consumer Consequences and Tools for Layered Defense.

How to Plan

This is where being proactive instead of reactive is crucial. Start with prevention and assume that at some point you will experience a breach – and not one that you're likely to discover. Most companies realize that they've been breached by a third party, as opposed to uncovering the breach internally.[7] Lack of dedicated internal resources and the increasingly sophisticated tools of data theft criminals make breach detection a tricky endeavor.

Here's what can be done now to help secure and protect the information your company is responsible for:

- **Segment sensitive data and restrict access.**
- **Wipe or shred physical media or paper**
- **Demagnetize external media and overwrite hard drive data**

Equally important as protecting your customers' data is outlining exactly what steps you'll take if or when a breach occurs. At the time of a breach, stress levels are high. There may be media scrutiny, and customers will want information. An outline with key players assigned to specific responsibilities will help eliminate errors. Build your company's 'hazmat' team in advance, including members with expertise in legal, public relations, compliance and risk management. Communicating effectively with both consumers and government officials should be done on a parallel path with securing the breach. In other words, both need to happen on the same timeline, so make certain in your company plan to dedicate adequate resources.

Take Stock Now

If you don't have the internal resources or know-how to cover the likely aspects of or fallout from a potential breach, call in a third party specialist to partner with your company through the breach resolution process. Having an expert on hand can help expedite the resolution, limit legal liabilities and increase customer satisfaction. Being prepared before a security breach occurs can mean a big difference to both your company's bottom line as well as the less tangible damage done to your company's reputation.

Assume that at some point, you will experience a breach – and not one that you're likely to discover.

To learn more about data breach resolution, visit www.Experian.com/DataBreach, or contact Experian® at DataBreachInfo@Experian.com or 1 866 751 1323.

7 **Javelin Strategy & Research** 2010 Data Breach Prevention and Response: Causes, Consumer Consequences and Tools for Layered Defense.