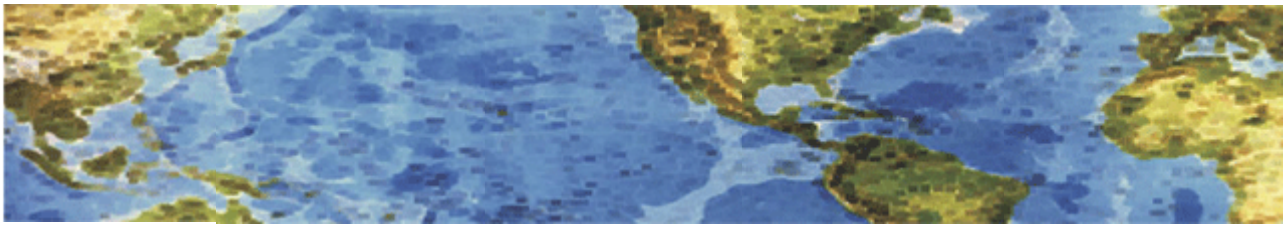
HALL ASSOCIATES



Risk-Based Decision Making Commentary
23 April 2014 Newsletter

Why Do Data Breaches Happen?

Wham—news of a data breach breaks. Updates flood the internet, accusations fly between parties, and everyone speculates. Why? How? What happens now? Amid the chaos and the hype, it can be difficult to get clear, accurate information about what's really going on when a data breach occurs. While data breaches are certainly a complex issue, equipping yourself with basic knowledge of them can help you to navigate the news, to handle the aftermath, and to secure your data as best as you can.

Let's get the story straight on why data breaches happen by looking at four common myths.

Data Breach Myth 1: Data breaches happen when someone at a company or organization steals data.

While the scandal of an insider hack seems oh-so-Hollywood, this is rarely the case. In 2012, according to an annual study by Verizon, 94% of data breaches were perpetrated by outsiders. These outside hackers may not even be in the same country as the organization they hack. Because most data breaches are not insider jobs, even organizations that you trust are at risk of having a breach. It's not as simple as picking out bad apple employees or avoiding sketchy companies. In fact, it's not only companies that need to worry about their data security.

Data Breach Myth 2: Data breaches only happen at stores where you make purchases.

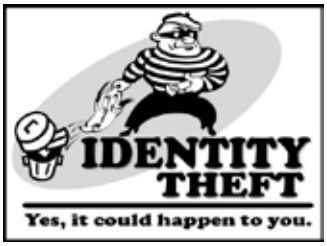
When you hear the phrase "data breach," what comes to mind? If it's Target, you're not alone. The magnitude of the Target Data Breach during the 2013 holiday season was unprecedented, with up to 70 million cards affected. The aftermath and press coverage continues even months after the incident. It's easy to see why large retail stores seem like the new face of data breaches. Yet, it's important to remember that all sectors are at risk of experiencing a data breach because of the value of data. Just look at Indiana University, University of Maryland, Yahoo, the state of South Carolina, and the California DMV, who all recently experienced data breaches. In fact, retail accounts for only 15% of all data records lost or stolen, according to SafeNet.

Hackers are not just after credit card numbers that they can fraudulently charge. Other sensitive information—name, email, address, or social security number, for example—can be sold or abused for a profit. It's important to use caution when you give out any of your data online or in person, and not only when you swipe your card.

Data Breach Myth 3: Data breaches happen every once in a while when there is a hole in security.

Data breaches happen all the time. A report by the Online Trust Association estimated that over 740 million personal records were exposed in 2013 alone, over the course of 614 breaches.

HALL ASSOCIATES



We don't always hear about data breaches because companies in some states are currently not required to disclose this information. In the aftermath of the Target data breach, Congress is attempting to pass legislation requiring timely data breach notification. Though data breaches hinge on exploiting a "hole" in security, this oversimplifies the problem. It's impossible for the average consumer to know the ins and outs of a company's security practices, and even if this information was made available, we could not predict what barriers hackers could break down to access valuable data. The real security hole is the poor standard of data security across the board.

Data Breach Myth 4: Data breaches happen because companies are careless.
The increasing frequency and magnitude of data breaches is a clear sign that organizations need to prioritize the security of personal data. Breached companies may be guilty of carelessness with private information, but we have to remember that the data breach game has an element of chance: many organizations that have not been breached are still gambling with user data by not ramping up their security standards. So while it's easy - and mostly justified - to point fingers at companies that experience breaches, it's important to remember these occurrences are symptoms of a larger problem. Collaboration between all sectors, including governments, banks, credit cards companies, retailers, and consumers, will be needed in order to raise the security bar.
http://www.abine.com/blog/2014/data-breach-myths-debunked/

An Oldie But A Goodie
I got an e-mail from a correspondent that just received a phone call from someone claiming to be a "Windows representative". She (the accent was possibly from India) tried to tell my correspondent that her computer was sending out a virus infecting other computers – and she needed to get signed on remotely to her computer to fix the problem. The correspondent would not allow that. She said she would call her local computer person but that made the caller mad. She then asked for the caller's phone number so the caller hung up. Interestingly enough there was a phone number on her caller ID – 215 area code. Assumption is that the phone number was spoofed.

No scam is too old/outdated enough for people world-wide to not continue to try it. The new scams simply build on older ones – these things never go away. So we need to be aware of all possible scams, or at least be aware of proper responses to any request for access or personal information.

HALL ASSOCIATES

Phishers Divert Home Loan Earnest Money

Real estate and title agencies are being warned about a new fraud scheme in which email bandits target consumers who are in the process of purchasing a home. In this scheme, the attackers intercept emails from title agencies providing wire transfer information for borrowers to transmit earnest money for an upcoming transaction. The scammers then substitute the title company's bank account information with their own, and the unsuspecting would-be homeowner wires their down payment directly to the fraudsters.

This scam was laid out in an alert sent by First American Title to its title agents:

"First American has been notified of a scheme in which potential purchasers/borrowers have received emails allegedly from a title agency providing wire information for use by the purchaser/borrower to transmit earnest money for an upcoming transaction."

"The messages were actually emails that were intercepted by hackers who then altered the account information in the emails to cause the purchasers'/borrowers' funds to be sent to the hacker's own account. The emails appear to be genuine and contain the title agency's email information and/or logos, etc. When the purchasers /borrowers transferred their funds pursuant to the altered instructions, their money was stolen with little chance of return. This scam appears to be somewhat similar to the email hacking scheme that came to light earlier this year that targeted real estate agents."

"It is apparent in both scams that the hackers monitor the email traffic of the agency or the customer and are aware of the timing of upcoming transactions. While in the reported instances, a customer was induced to misdirect their own funds, an altered email could conceivably be used to cause misdirection of funds by any party in the transaction, including the title agent themselves."

This scam is almost certainly not unique to First American Title; scams that work against one corner of an industry generally work against the industry as a whole. Attacks like this one illustrate the value of two-factor authentication for email. The larger providers have moved to enabling multi-factor authentication to help users avoid account compromises. Gmail.com, Hotmail/ Live.com, and Yahoo.com all now offer multi-step authentication that people can and should use to further secure their accounts. Dropbox, Facebook and Twitter also offer additional account security options beyond merely encouraging users to pick strong passwords.

http://krebsonsecurity.com/2014/04/phishers-divert-home-loan-earnest-money/