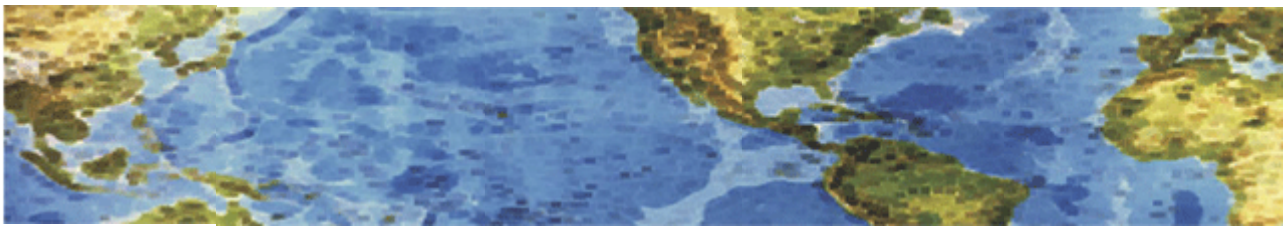
HALL ASSOCIATES



Risk-Based Decision Making Commentary
2 January 2014 Newsletter

Lessons Learned (Hopefully) From the Target Data Breach

Target confirmed on 19 December that it's investigating the theft of credit and debit card numbers from millions of customers who shopped at its stores over the past three weeks in what may be one of the largest data breaches ever. The company says that card numbers, expiration dates and CVV codes -- the three- or four-digit numbers printed on the card to provide extra security -- may have been taken from as many as 40 million people who shopped at U.S. Target stores between November 27 and December 15. People who shopped online or at Canadian Target stores were not affected. The company hasn't released details other than malware infected its point-of-sale system, but the United States Secret Service confirmed to USA TODAY that it's investigating the Target data breach. All types of cards were affected, including Target's own REDCard credit cards. The company has posted additional information for customers and says it's confident that data is no longer being stolen.

Security journalist Brian Krebs has confirmed that stolen credit and debit card account numbers are appearing on black-market websites in batches of 1 million cards and selling from $20 to more than $100 per card. Interestingly, several banks have actually bought back large clumps of their credit cards from these online stores. Following the announcement that 40 million credit and debit card numbers were stolen from people who shopped at Target stores between November 27 and December 15, some card issuers and customers are now detecting illegal use of those accounts by identity thieves. In response, many banks and credit card companies are saying that the fraud is being investigated and that customers will not be responsible for fraudulent charges.

The US Department of Justice is now investigating Target's data breach and federal lawsuits are coming in from customers around the country. By December 22, more than a dozen Target customers had filed federal lawsuits, with some accusing Target of failing to protect customer data. At least three class-action lawsuits have already been filed and several states are looking at filing lawsuits. In addition, banks and other financial institutions could (and probably will) sue Target over this breach. Financial institutions have sued merchants after data breaches in the past. One area of ongoing litigation is who actually pays for fraudulent charges on these cards. Customers will not be held liable but there are plenty of others – financial institutions, card issuers, insurers, point-of-sale companies, merchants, etc. That will keep litigation going for years.

In addition to the legal and possibly criminal complications from this, Target is also having to deal with the public relations fallout. Before this incident, the Target brand's consumer feedback index from one survey dropped from 26 (a fairly good score in this survey) to a negative 19 in only a few days. And there are plenty of anecdotal interviews with people who "plan to stop shopping at Target".

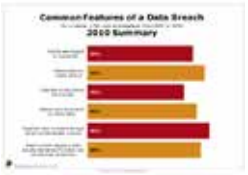
HALL ASSOCIATES

The first lesson learned is that NO ONE is totally secure online. No matter what is done, what security apps you have installed, how much protection you or your business has, your personal and business information is at risk through your devices, systems AND your use chain. We need to focus on the growing problem of financial data theft. Keep in mind: Target was just one of about 600 publicly disclosed data breaches in 2013. There are tens of thousands of criminals all over the world working on getting and using your personal and business information FROM ANYWHERE for gain – and NO ONE should consider themselves "safe" because they are only a small part of the crowd. Do you know where your personal and business information is and how it is protected? Note that the U.S. is the juiciest target for hackers hunting credit card information. And experts say incidents like the recent data theft at Target's stores will get worse before they get better. That's in part because U.S. credit and debit cards rely on an easy-to-copy magnetic strip on the back of the card, which stores account information using the same technology as cassette tapes. In most countries outside the U.S., people carry cards that use digital chips to hold account information. The chip generates a unique code every time it's used. That makes the cards more difficult for criminals to replicate. So difficult that they generally don't bother. The U.S. is the top victim location for card counterfeit attacks.

Second lesson learned is that you need to continuously monitor your accounts, both individual and business, since you cannot know when and how account or identity information is stolen. The best we can do is be prepared to notice as soon as possible (basically report suspicious transactions/ requests immediately) when something is wrong with your accounts/identity and **know what to do and who to contact** to stop any activity. Look at credit/debit card accounts daily, look at your credit reports at least three times a year. A credit freeze is the smart thing to do if social security numbers are stolen (did not happen in this case), as that can prevent an identity thief from opening new accounts in your name. As a precaution, I recommend that you lock your credit account and have one of the credit bureaus monitor your credit and accounts. It would also be useful to sign up with one of the several available identity theft protection companies – much like you use a security company to protect your home and/or business. Also use antivirus/antimalware applications on all of your devices/systems and networks.

Third lesson learned is ensure that you have done all possible to make it harder for criminals to use any information they do get. If you have a large/business account, work with the financial institution to set up a profile of possible transactions and a dual authorization scheme. If anything outside of your profile is requested (such as an overseas wire transfer) then the financial institution will know to notify you first. If you maintain personal or account information on your devices/system, then ensure that **all data AND communications channels** are encrypted. Encrypting your data bases does little good if you send personal or account information around in the clear (say by e-mail). Good encryption will make it very hard (if not impossible) for anyone to use data gathered from your devices/systems.

HALL ASSOCIATES



Fourth lesson learned is to understand who has your data and how they protect it. In many cases (Target, for example) you cannot simply request that they answer questions about their security practices – at least not yet. But you can request answers from your financial institution, your point-of-sale company, the company that runs your web site, etc., all areas where your individual and business data may be.

Fifth lesson learned is about debit cards - Target confirmed that encrypted PINs were stolen in the breach, though it said the "key" necessary to decrypt data is not within its system and could not have been taken during the breach. Changing your PIN will prevent a stolen debit card number from being used to withdraw cash at an ATM, but it won't stop a crook from using it to buy things. Debit cards can be used without a PIN at most stores. To be completely safe, you'll need to ask the bank to issue you a new card number.

Sixth lesson learned is that scammers will take advantage of **anything** to try and get your personal or business data. We have already seen e-mails supposedly from Target or a law enforcement agency requesting “additional information about you so they can monitor your accounts”. Beware of email alerts that ask you to provide your personal information. Target is not doing this, and no company or government agency would. **These bogus alerts are from identity thieves.**

Seventh lesson learned is how not to respond to a data breach. Target shows how **not** to respond in a crisis. Although they have done many things right in their response to the second-largest retailer data breach on record, they have made some classic mistakes that have not only compromised their reputation, but the trust of their customers, employees, and the public. To be fair, almost certainly Target did not know all the facts when they had to make their initial statement on December 19th (the story was broken on December 18th by security blogger Brian Krebs, “Sources: Target Investigating Data Breach.”) But **because they had chosen not to break the story themselves**, Target was forced to respond to a story that Mr. Krebs had broken, and from that point on they were on the defense. And, in such circumstances, they were most likely buffeted by conflicting “advice” or demands from their security experts, banking partners, law enforcement of every variety, and lawyers. Many of Target’s crisis responses were textbook good, but what they forgot was to NOT make assurances to the public until they were certain those assurances were correct. They were far too quick to worry about the spin, and minimize the problem, instead of admitting the things that they did not yet know, and plan for the worst case. Indeed, Target leadership’s biggest flaw may have been to listen to the wrong experts: they stayed silent when they should have broken the story themselves and over-communicated. They minimized when they should have maximized. They obfuscated when they should have leveled with their customers. And they made false assurances that they later needed to retract. Now, fewer will believe them when they speak. And there is more fodder for court cases. Following are 7 things businesses should do in cases like this to minimize the public relations and possibly the legal fallout.
(From Forbes Magazine - http://www.forbes.com/sites/daviatemin/2013/12/30/targets-worst-pr-nightmare-7-lessons-from-targets-well-meant-but-flawed-crisis-response/)

HALL ASSOCIATES

1. Business leaders, no matter how much it hurts, when you have a problem that affects your customers directly, **DO NOT WAIT TO GO PUBLIC**. You don't need to have all the answers, but you DO need to get ahead of and own the problem. Otherwise, others will own it for you. Announce what you do and do not know as soon as possible, make clear your intentions to come up with solutions as rapidly as possible, and promise continuous updates. Then keep to that promise. Your business will definitely take a major hit, but your credibility will not. And if you keep the trust of your customers, your profitability can rebound.

2. **Do not let others define your message**. Law enforcement, lawyers, banks, and security experts will all want to craft your messaging for you. Hear them out, of course, but then do what YOU think is best for your customers, employees, and shareholders. There may be a dissonance, because what is best for customers may not be best – in the short-term – for shareholders. But above all, guard your integrity, and show ultimate respect for your customers. If I have heard one regret from CEOs in this position, it is that they listened to the wrong advice, and waited too long to step out with their voice in public.

3. **DO NOT make false assurances**. One simply cannot make assurances to the public unless you are 100% certain those assurances are true. Just like UPS and Fedex promised on-time Christmas delivery this year, and then couldn't deliver on their promise, there is nothing better to destroy trust than making an assurance one day that you will have to go back on the next. It is far better to be criticized for being uninformed than for misleading the public.

4. **Don't let the bad news dribble out**, if you can help it. Almost all crises are multi-day, or weeks or months long. If you can get the bad news out as quickly as possible, you can then turn to what you are doing to address the situation, and recover.

5. **Respond forcefully, and commensurately with the problem**. Target's response on its website has many admirable elements, but it is still too little, too late. Given the scope of the problem (40 million customers we know of to date), it is far too general. It doesn't address the broad array of issues resulting from the theft anywhere near enough, such as what Target is doing to stop these kinds of abuses from happening again, or how fraudulent use of a credit or debit card will affect a customer's credit rating, and what can be done about that. The list of important things to know that Target includes on its website is excellent, but I would be clearer on the specific things customers can do to protect themselves (such as get a new card), and offer to help them do so. After all, criminals often sell stolen card numbers months after their theft, and the best thing to do is not only change your PIN, but get a new card.

6. **Balance "happy talk" with "straight talk."** If the problem grows and your response stays in the sales mode, you run the risk of being totally unbelievable. In a crisis, straight talk is usually appreciated. Only AFTER the straight talk can you find something to be happy about.

7. Finally: **Never, ever say you are "taking the issue seriously!"** Of COURSE you are, if you are any kind of a leader at all. That is the floor, not the ceiling. Instead, give specifics. Talk about the steps you are taking to fix the issue. Tell the story. Talk about your values and vision, and how you are living them in the wake of the crisis, no matter how difficult that may be. Reinforce your commitment to be a part of the cure.

These are all ways for organizations to stay close to, and sympathetic to, their audiences in the face of crisis. Make sure YOUR concerns directly reflect the concerns of your customers, clients, employees, and stakeholders, then you will have far more willing partners in your recovery.