8-Forbes-The Target Data Breach

Target

data breach have continued to emerge. It’s not a pretty story. Bad enough when it appeared that through some means, hackers had gotten data all the way from credit card swipe machines out the other side of Target’s systems, including encrypted Pin numbers from debit cards. Then it was announced that other information was also stolen, specifically name, address, phone number and/or email address. I assumed this was all somehow related to the same attack. Perhaps a different database, but all information gathered from those who shopped from mid-November through mid-December 2013. Then last night (like colleague Claire O’Connor), I received my copy of “the letter.”

In case you haven’t received one, I found a copy of the letter online at marketplace.org. It’s identical to the one I received. This is a very significant letter, especially addressed to someone like me, since I haven’t shopped at Target stores in recent memory, and possibly shopped at Target.com over a year ago. In other words, the data captured was far broader than we originally imagined. This is bad. *[Worry]*

Other details emerged Thursday about how the breach occurred. Until then everyone, including me, speculated wildly about how this could have been done *[Worry]*. And we focused on one point of attack – the POS system. There are standards retailers follow, set forth by the payment industry (led by

Visa

) that are meant to keep data safe. But it turns out that if a bad guy can break into the corporate system itself, all those standards are pretty useless. And that’s what happened. If you’re feeling particularly geeky, you can read an excellent explanation of the attack here , at www.krebsonsecurity.com. I’ll try to give a simpler overview for the rest of us.

The software used to hack the POS system is a variant on one that is commercially available on Cybercrime forums (note: Seriously??? Cybercrime forums? And our governments allow those forums to continue?), for the robust sum of $1,800 for the “budget version” and $2,300 for the “full version,” which also allows the bad guys to encrypt the data they’ve stolen. *[Anger]*

This is bad enough, but the real question remains – “How did they gain access to Target’s systems?” And they didn’t gain access just once. In fact, they kept coming back to harvest data almost daily over the course of several weeks. *[Disappointment]* As we now know, they didn’t just stop with the sales data. They roamed across Target’s network of servers looking for interesting information, like email addresses, etc. *[Disappointment]* The answer is apparently found in what is known as “Port 80.” Let me try to give you a layman’s explanation of this.

We have software firewalls on our personal computers (if you don’t, you really should). This is the software that warns you if you’re being directed to a malicious web site. It also insures you don’t get malware planted on your computer if you somehow find yourself on one of those, or get an email with that type of software in it. Large enterprises have both hardware and software firewalls designed to do essentially the same thing, just on a more robust scale. The software and hardware essentially seal up all ways in and out of your computer – except for a very few exceptions. One of those exceptions is the route (or “Port”) used for internet browsing traffic. You can’t close it – not if you want to use the internet. So we rely on software to separate bad apples from the good ones. Long story short, the hackers convinced Target firewalls that they were “good guys.” And once they’d done that, they continued to roam freely around Target’s system. They’ve found data old and new and will use it the way they choose.

Personally, there’s not too much they can do with whatever data they got from me. I haven’t shopped at Target in a long time, and they have no credit card number info on file. But imagine if they grabbed not just your credit card swipe information, but were able to match it up with the other information: address and phone number info as well. They could do a LOT of damage. And that probably explains why finally, banks like Citibank announced they were re-issuing all debit cards that were possibly involved in the breach. It's no longer adequate to just change the Pin numbers. Now, it's a do-over. I think this was a wise move. As I've mentioned before, I'm frankly pretty befuddled that the entire ecosystem did not move faster to replace cards, change Pin numbers…whatever it took to keep us all safe.

And that brings me to the last point, one that is worth consideration. Retail industry watcher and former National Retail Federation CIO Cathy Hotka points out that most industries have cooperative security groups, called ISACs (Information Sharing and Analysis Centers). If you look at web site www.isacouncil.org , you'll find many industries participate this way. When something bad happens, they share information. Retailers, for some reason, have chosen not to create this type of group despite potential assistance from US-CERT, the FBI and other enterprises. Cathy (and now I) expresses real befuddlement over this gap. There's plenty of precedent. Retailers routinely work together on loss prevention tools and techniques, and lobby hard for more assistance from law enforcement against Organized Retail Crime (ORC). It seems that it's long overdue for the industry to do the same when it comes to Cyber-security.

I can appreciate why retailers wish this issue would just go away. After all, they've each spent a small fortune on Visa's PCI compliance initiatives. *[Positive]* It's a hard pill to swallow that a static standard is inadequate in an ever-changing world. And now, there's a belief that moving to a new technology that will replace today's magnetic stripes, called EMV, will solve any remaining problems. The Target breach highlights that there will be no magic bullet. The bad guys will continue to evolve. We must do the same. *[Positive]*

Consumers have grown weary of privacy invasions. This more than anything, explains the surprisingly vocal reaction to the Target breach vs. the TJ Maxx data breach some years ago. Retailers are in for challenging times again. It would be best to see us working together to stay a step ahead of the bad guys.

And seriously…can't we find a way to shut down the cybercrime forums? It's a better use of time than tracking every phone call we make. Really.