All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

What's the big deal about big data loss (actually theft)?

I get confused about the way security deals with so-called data loss (actually theft). Recently we had what the media called, in various forms, a crisis, a huge cyberattack against, and so forth against JPMorgan Chase, one of many such instances in the last year. So I looked at the various claims surrounding this instance, and found consistently that the only known “loss” of data was names, addresses, phone numbers and email addresses. And it wasn't lost! It was stolen, and JP still has copies. So to be really clear, this is more or less the same information found in the phone book, available from various mailing list providers for less than a tenth of a penny a piece, and of no significant consequence I can identify. The cost of “protection” for consumers is $90 per person per year, although I don't quite get what this cost covers.

It's all about the spam?

For some reason, the claim out there is that the stolen information may be used for “phishing” (a strange term of art that means using email to lie to people to gain information) or “spit” (a stranger term indicating spam over VoIP – don't ask why it's not “spoip”). While it's true that you might be able to better convince a few folks that you are legitimately from Chase with the knowledge of this information, it is also true that I have been getting Chase and JP Morgan spam for years, none of it from them, and none of it effective. I don't think the fact that they know my name, address, and phone number along with the email address they use is likely to be effective at convincing me of anything meaningful. But if it did and they wanted to know it, they would only have to look it up using a legal search – for a few cents per record at most.

And they are not alone

In September, Home Depot revealed that it had information related to 56 million debit and credit cards stolen. The Target data breach supposedly leaked details on 40 million credit and debit cards. TJX had 90 million records or so taken in 2007. The list goes on and on. Some are worse, facilitating some level of fraud by revealing credit card and debit card details that might be exploitable because of the strong desire to let money flow wherever possible (i.e., to make more sales by making buying easier). They steal money from the credit card system, which charges fees to compensate for such losses. Some are not as bad, revealing only information that was already readily attainable by looking it up on the Internet – like Chase.

Of course it is not a good sign that one after another major retailer and bank falls prey to distant threats taking advantage of weaknesses in systems, methods, and people; entering and gaining control over limited portions of their information infrastructures. It's even worse that they seem to keep enormous aggregations of data in one place, putting all their eggs in one basket so to speak. Some of the attacks are identified as clever because they enter through a path not previously publicized in the media (i.e., point of sale, air conditioning, or other system). But in truth, it's the same old attacks we have seen for more than 20 years.

And it seems like it is getting worse, even though no real facts seem to support this claim in a meaningful way I can yet understand. At some point, of course, all of the data will have been stolen and published over the Internet, and there will be nothing left to steal. Hmmm...

And yet here we are

In the US, there are about 350M people. Once all of them have their “personally identifiable information” stolen, is all the liability gone? Think about it. What if we paid annually as a country? 350M*$90=$31.5B/y for full identity theft insurance for every person in the US. The US losses from identity theft are less than that, or insurance couldn't cover it. The US GDP in 2013 was about $16.7T, which means this would cost less than 0.2% of the GDP. At some point, we can simply assign a value to protection, charge protection prorated to those with the data, and end the fuss. We could even make all the data public and demotivate the break-ins!

But risk aggregation issues, imperfections in defenses, and protection costs aside, I am having some difficulty understanding why we care so much about this. The fear mongers seem to be telling us that something dire is happening. But I don't really see it. I live a life like many others. I work a lot on computers, use email, social media, and VoIP/cellular to communicate. I use credit (not debit) cards to make most of my purchases. I have personal data, health data, pictures of travel, my calendar, etc. online. I drive a car, buy clothes I like, go out to meals sometimes, get cash at the bank, go for walks, play music, watch cable TV, read, write, sleep, move stuff, make dinner (more often eat what others have made), etc.

And it seems to me that **things are better now** than 5, 10, 20, 40, and 50 years ago.

Despite the fear mongering about the dangers of cyber attacks, far more people have and use cell phones today than 5 years ago, they do more things, cost less, are more reliable, easier to use, and you get more for less. They are imperfect, of course, and we complain about the poor service when driving through a tunnel along the coast and the horror of limited bandwidth to only a few gigabytes per month for less than $50 with unlimited talk and text.

But wait a minute... when I was growing up it was land lines only, and they were noisy at times, there were phone outages from time to time, and each local call was 10 cents, with long distance running more like 10 cents or so per minute. My first cell phones (I had two at the time) were the size and weight of a brick, had 5 inch antennae, worked only in limited urban areas, charged from 20 to 50 cents per minute for every minute PLUS long distance charges, only made phone calls, ran for about 2 hours on a battery, and required extensive credit approvals. That was about 30 years ago. In the late 1990s, things got better, cheaper, and faster. As they did in the 2000s, and as they are doing today.

And we have or are about to have widespread digital wrist watches with health informatics, email, calendar, etc. built in, integration of a wide array of different data from many millions of sensors for details of all sorts of things ranging from prices to weather to traffic to locations of nearby friends and acquaintances, controlled by voice input, running for days to weeks at a time on a single battery charge, with high definition video cameras and output, voice input that works for many tasks, water resistant, hard to break or scratch, very light weight, easier to use, harder to steal, with more data, speed, input and output capability, etc. than ever.

My credit cards are less expensive than they were 30 years ago, purchasing is easier and faster, I get instant notification of purchases via cellular often before I have to sign the receipt, I can buy more and better things for less money, faster, have them delivered for almost nothing in very little time, more reliably, tracked, and they almost always show up in great shape. My car is more reliable than when I grew up and getting even more so, it is more fuel efficient, faster, better handling, safer, more comfortable, and less expensive for what I get.

Back to the data

All of this may seem irrelevant to the issues of data theft and break-ins. But to me they are exactly the point. I am not afraid of the present or the future. Things are better off now than they were then. And they are getting better still. We are concerned about a few people being killed here and there, and that is a good thing to be concerned about. But when I was growing up we were concerned about nuclear attacks killing most of the humans on Earth in a few hours. Tens of millions of people were killed in a few years in World War 2.

We talk about losses potentially (not actually) affecting tens of millions of people. The effect in most cases is that you get a new credit card in the mail in 6-10 days and have to use another credit card in the meanwhile. You may have to tell your regularly scheduled automatic payment systems about the change. Your financial loss is likely nothing at all, but it could go as high as $50, unless you used a debit card with a bank account with a lot of cash in it, in which case you should learn to only use credit cards. And even debit card frauds are largely covered today as far as the consumer is concerned.

You do have to check your monthly statements – if you still get them on paper. Or you could check each transaction as it occurs with the automation. Big deal! You always had to check statements for credit card frauds, wrong charges, returns not credited, duplicated charges, etc. That's the price of the extremely convenient life lived with information technology.

Ebola is scary. Of course it is. It is a disease that could kill millions or billions, left unchecked. But it is checked. The checks are imperfect of course, it has killed thousands in the last few months, and could reach millions. That's just nature at work. The influenza epidemic of 1918-19 infected about 20% of all humans, killing about 2%. Other diseases kill millions of people each year. But information technology is helping us reduce the effects, come up with cures, track the cases more quickly and reliably, do better analysis, sense conditions likely related to ebola, do better, faster, cheaper tests, and support the logistics required to effectively limit the ultimate effects of this and many other diseases. We live better longer because of the data.

We still have nuclear weapons, and while we have fewer of them than we did at one time, they can still kill all of us in a matter of a few hours (even though some of us may live for a few months or years before we also die). Information technology plays a very significant role in keeping track of these weapons, but perhaps more importantly, in reducing proliferation, tracking nuclear material and components, detecting potential future use, detecting advances by those wishing to attain such weapons, and apparently preventing (stuxnet) some (Iran) from getting them as soon as they might otherwise have.

Data is a good thing! Information technology is a good thing!! More data and technology is a good thing... for the most part and most of the time. But, like any other technology, information technology is a two-edged sword.

I get it - of course...

We want to do better. And we should. And we are! Things are better than they were and getting better still, for most of those living in modern societies. But as we create increased benefits and value associated with information and related technologies, we also come to depend more and more upon it. It's obvious that we have serious challenges facing us in the information protection arena, and that we are far from the ultimate goals we hope to reach, as in every other area of human endeavor. But fear is not the way to move this ball forward.

Even more importantly, our society seems to always emphasize the irrelevant. JP was right to point out that no customer accounts were affected and there was no indication of frauds against those accounts (beyond the everyday ones unrelated to the data issue). The big story here is that none of the really bad consequences of attack appear to have been at issue. The bank did properly protect the critical data and the criminals only got to what is largely public information. Name, address, phone number. All information from the phone book we access for free over the Internet and used to have in paper in every house in every city.

Credit card numbers and related information hardly reaches the threshold of importance that justifies widespread fear. In the other criminal acts we hear about, essentially all of the actual losses are from adding protection for frightened customers and reissuing credit cards, which have to be reissued periodically anyway. So the net real effect is likely on the order of a few cents per customer for Chase, more for others who had to send new cards out.

In other words, big data theft is really no big deal.

The big deal would likely come with an attack that scrambled bank balances, perhaps by doing millions of electronic funds transfers, inter-account transfers, or just randomizing the current balances. But this is not data theft!

So you know, most large banks don't use the same sorts of systems for tracking money in accounts as they do for storing credit card numbers, names, addresses, and so forth. They tend to use transaction systems. Transaction systems typically include multi-site redundancy and sequentially track every transaction in a way that is hard or impossible to erase later. The net effect is that even if someone sent a phony transactions into the systems, and even if these transactions went through, most of them could be unwound very quickly, and some of them would take longer, but get done in weeks at most. It would be expensive to get the last ones right, but it would get done, with the help of customers and lots of extra effort. Or perhaps some small number of people would not be made whole and would have to sue. But the point is, the effect would not be catastrophic except to very few. And as a society, we tend to tolerate this level of loss. We would like to do better. We want to do better. But so it goes.

An even bigger deal might be an electronic funds transfer of a few hundred billion dollars to a bank in Syria over which there was no control or recourse. But again, this is not data theft!!

This is also hard to accomplish, and I bet it would be unwound by the Federal Reserve in an “unusual move”. That's because, in addition to a technical system, we also have a human system. As a society we are unwilling to allow our rules to get in the way of our well being, because that's why the rules were made; for our well being; or someone's well being. In any case, you can count on really massive damage being undone by people and organizations taking control over their computers, to the extent they can.

Then there is the physical damage from cybernetic systems where computers controlling the feedback mechanisms are connected to the Internet and caused to malfunction. It's possible, it's feasible, it has happened. But again, this is not data theft!!!

Summary

To really understand these issues, you have to dig deeper. When you do, you find that data theft is not the biggest issue we face. It doesn't produce the losses that corruption, service denial, uncontrolled use, and lack of accountability, transparency, or custody might. We don't like it, it's inconvenient, and companies should stop it. But **big data theft is no big deal!**