Valuing Secure Access to Personal Information

by Ben Malisow
last updated August 19th, 2004

Securing data is not a simple endeavor; a multi-discipline, defense-in-depth approach is necessary, as information can leak at any point in the communication process, from receipt, through storage, retrieval, transmission, and so on. Furthermore, each information system element is vulnerable to loss, including hardware, software, and personnel. Add to this the exceptional efforts made by those who want to acquire information through illicit means, whether for espionage, criminal, political, mischievous, or other intent...someone is always trying gain access to information they shouldn't have.

Organizations, for the most part, have come to recognize the value of the operational and functional information they possess, and are taking pains to protect it accordingly. This might be because of legislation such as the Health Insurance Portability and Accountability Act (HIPAA), which mandates better security processes, or because of every-increasing case law findings against organizations that don't do enough to protect their own vendors' and customers' data, such as the decision earlier this year against the U.S. Department of Interior for not maintaining adequate control of Bureau of Indian Affairs databanks. Or it could be a simple recognition of the growing threat of security issues, leading some entities to act unilaterally to protect information under their control.

But what about the personal information of individuals? Are the protections afforded to other types of information increasing apace for the data pertaining to a single person? What about identity theft?

More importantly, do we, as individuals, recognize the true value of our personal information simply as personal information? Sure, most people understand why distributing their credit card information, or ATM PIN, or Social Security number is a bad idea, but do they understand that their most basic personal information now has an inherent value?

We've reached the point where information has an integral value of its own. Do governments acknowledge this modified nature of information? Does the commercial world? Do the individuals themselves understand that their own information is valuable for no other reason than that it is their information?

A case of personal information leakage

To examine these questions, here is an overview of one type of information transaction: an American consumer, resident of the Commonwealth of Virginia, going through the process of renting an automobile from the Hertz agency, over a cellular phone, using an American Express card.

This simple process involves calling the Hertz toll-free reservation line, to speak with an attendant who transcribes all the pertinent rental information: the time, place, and date of the proposed rental and return of the vehicle; the customer's name, address, telephone number, e-mail address, and billing information; and whatever sundry other items that comprise the transaction, such as coupons, etc.

There are two obvious risks to the customer's information apparent in the process at this point, and two more subtle risks.

The first two are the means used to transmit the personal information (the cell phone), and the person taking the information. While cell phones are notorious information-leaking resources, the ubiquity of their use and the sheer volume of calls makes it an impractical medium for eavesdroppers, and damage and liability would be very difficult to assign to a mobile phone service provider. Similarly, the risk incurred by sharing your information with the Hertz (or any other car rental company) reservation representative is attenuated: trying to reduce risk by mistrusting all personnel involved in commercial transactions would just render the use of credit cards or other fluid monetary tools useless. You have to trust somebody, which often results in trusting either everyone or no one. The true risk of this is minimized by legislation pertaining to credit transactions: credit card customers are liable only for a certain amount (usually $50 US) of illicit billing from a compromised credit card account.

The other two, less distinct, threats arise from the vagaries of an individual company's policies, in this case American Express, and a unique Hertz company practice for obtaining a customer's driver's abstract. The issues in the example, however, can be applied to many

others.

The American Express company's security practices, like those many companies, may be cause for concern. American Express has elected to provide its customers with e-mail and Web communications concerning their accounts, in the interest of both enhancing convenience and reducing their support cost. This, in and of itself, is neither good or bad in terms of security. The risk has come in the form of the American Express' security response to e-mail social engineering attacks.

Consumer e-mail scams

E-mail scam threats (including financial "phishing" scams) exist for almost every type of consumer transaction, so it is not atypical for American Express to face this type of attack. The company's response, however, to the threat may be somewhat lacking. If an astute reader receives an e-mail scam purporting to be from American Express, or any other financial organization, it is often very difficult to make the company aware of it. In contrast, notifying the company's security division of a lost or stolen credit card is extremely simple: it is even one of the main options listed on the initial telephone key menu at the beginning of every call to the American Express customer service line.

The contact information for the security office is not readily listed on the American Express customer website; there is no apparent direct telephone number to report an attempted theft of personal information (there is, however, a fraud prevention and data security line for merchants, as well as an emergency card replacement line for corporate customers). Under the "Contact Customer Service" web-based e-mail section of the website, there are several subject lines listed- none of which deal with security concerns in any way. Unfortunately, this sort of practice can be commonplace amongst large financial companies.

Should a customer take the extra steps to contact customer service representatives and asked to be transferred to the security division, there is often still no hope that e-mail threats will be treated seriously; the security division of American Express claims to have no capability to receive forwarded e-mails containing scam information, and, instead, asks that a printed copy of any suspicious e-mails be faxed to their offices.

Of course, there is a reasonable amount of sense in this approach: if American Express, or any other financial company's security department, were to accept external e-mail, the company itself would likely be inundated with attacks of widely disparate validity and potential damage. And if the company tried to track down each and every spam-like e-mail scam attack on its customers, the American Express security personnel would have time for little else, as it could be an unending task. From a business perspective, it is best for the company to respond only to those instances of actual theft, where it can readily respond by closing the account, assigning an investigator, and working with law enforcement to find the perpetrator(s) by beginning from the point of sale where the illicitly-gained credit information was used, or the delivery location of the goods or services acquired thereby.

From the perspective of security for the personal information of individual cardholders, however, this is not a very proactive approach, and is akin to closing the barn door after the horses have already fled.

Your driving record

Continuing with our car rental example, Hertz has opted to decline rental service to those persons who have a questionable or negative driving record. This is understandable from the company's perspective -- who wants to give a car to someone who has a substantial history of running down pedestrians? As a discriminating vendor, Hertz reduces its own liability, costs associated with legal fees for recovering damage to their vehicles by careless or poorly-skilled drivers, and, perhaps, even insurance underwriting costs.

Still, it would seem that allowing Hertz personnel to access this type of personal information would cause undue risk for Hertz customers. Hertz, however, appears to understand this, and has taken great pains to not only divest itself of inherent liability, but to secure the transmission and receipt of this data as much as possible.

Richard Broome, Vice President of Corporate Affairs for Hertz, is quite clear about acknowledging the company's responsibilities. He states, "I think the important points here are that we are dealing with public information that has very restricted access within Hertz and is subject to both internal procedures and the company's privacy policy." All elements of this statement are reassuring, as is the process itself.

Hertz contracts a review of an estimated 90% of their customers' records, using a third party, information vendor TML, to conduct the actual search and interact with the Department of Motor Vehicles (DMV). Hertz gives TML a list of criteria to approve/disapprove a driver; TML makes one-time contact with the DMV for each personal record, and does not store the information. This process is relatively secure, and does not compromise an individual's security. But there is one troubling aspect to this transaction, involving the state of Virginia itself.

Virginias statutes allow rental car companies and their agents (such as Hertz and TML) access to DMV records. Virginia code § 46.2-208 also allows access by any other private entity which, "in the conduct of its business," submits a request for access. This same statute prohibits Virginia residents from accessing any of the same information, unless it's their very own record. Thus, it is arguable that the state's legislation suggests that companies are trustworthy, but Virginia's citizens aren't. More important, however, is what happens to your personal information and the inherent value thereof: your personal information, you driving record, is sold for a profit.

According to Theresa Gonyo, spokesperson for the Virginia DMV, that organization has 2,144 active business and government customers which purchase personal driver information; in fiscal year (FY) 2003, sales of Virginia DMV records grossed over $31 million (US). The statute that enables businesses to purchase private information cites another Virginia statute that stipulates that all monies generated by the sale of such information "shall be set aside as a special fund to be used to meet the expenses of the Department [of Motor Vehicles]." In 2003, however, the General Assembly decided to transfer some $10 million (US) into the state's general fund. The state has therefore gone into the business of marketing and selling its citizens' private information for the purpose of funding the state government. Nowhere on the driver's license application is it clearly stated that the applicant's information may be sold at a profit.

Other states, organizations, and companies in the United States clearly have similar policies and processes, whereby they can profit off a consumer's personal information.

Personal information is commonly sold

The above example is not unique to Virginia, or even to government entities as a whole. In almost every financial transaction where consumers freely part with their personal information as a means to gain market advantage (loan requests, mortgage paperwork, credit card applications, magazine subscriptions, etc.), that information is inevitably sold by the entity to which it was provided. The question is certainly not whether this practice is legal, moral, or ethical, as the consumer has voluntarily (even happily) surrendered this information for sale in order to gain something; the question, instead, is whether or not consumers fully understand not only the value of their own information, but the risks associated with that data because of its inherent value.

If consumers were to appreciate the value of their own information, and the threats to themselves as individuals in case of loss, inadvertent disclosure, or abuse, would they demand much more reciprocal value in return for having shared it? Jim Webster, an IT security consultant in the Washington, D.C. area, puts it this way: "This is the rationale I use in accepting Safeway's 'discount' card: they [Safeway] get to learn about my purchasing habits and I get a discount on products. You can argue whether the exchange is equitable, but at least there is some level of compensation for the surrender of personal data."

In our example, Hertz gets something of value to the company (information which allows them to avoid customers with higher risk quotients), TML gets something of value (money from Hertz), and the state of Virginia gets something of value (money from TML). However, the ostensible owners of this information (Virginian drivers) get nothing immediately tangible in return -- no rebate from the state from the sale of their information, no discount on drivers' license renewals, no discount from Hertz when renting a vehicle. In fact, it's very likely that most drivers aren't even aware there is any inherent value in their driving record and driver's license.

It's important to note that Hertz, TML, the state of Virginia, or American Express are not culminating any grand plan to exploit the value of your information....The point, instead, is that this practice is already common in much of North America, and indeed many other parts of the world; organizations already know the inherent value of personal information, while individuals don't.

Security starts with you

Those in the security field always seem to assume that someone, somewhere, does the job much better than their own organization or client. This might be because the bane of security professionals is never having enough resources -- time, budget, personnel, management support -- to secure the organization they serve to an "optimum" posture; there are no security providers that believe that their organization has been completely secured.

Few instances so dramatically demonstrate this attitude than the steadfast assertions by those who work in the public and private sectorsthat each other's clientele are somehow more serious about, or effective in, providing security. Is this truly the case? Does the Department of Defense somehow secure their systems better than Citicorp? Is Amazon better-secured than the U.S. State Department?

The particular example used in this article might give credence to the fact that no specific type of entity, public or private, is especially better or worse at securing personal

information of individuals. American Express, a private company, may be lacking some concern about its customers' security. Hertz, the sole rental car company that requests driver record information from the State of Virginia, creates situations where risk and liability, while attenuated through effective security practices, is increased during rental transactions. The state of Virginia shares private consumer information with just about anyone who wants it -- except its own citizens -- in what is, granted, a fairly secure fashion.

Why, then, should this type of transaction, or even the concept of information-sharing among entities, public or private, be of any concern to consumers? Aside from issues such as identity theft and other criminal activities, your personal information on its own merit, is still valuable. Consumers, even educated, modern consumers, often do not appreciate the value of their own information.

In the opinion of the author, such awareness is inevitable and necessary. From the Agrarian and the Industrial ages to today's Information Age, at each historical juncture people were forced to acknowledge that previous value systems had changed, for good or ill, and that new opportunities and responsibilities were available to them as individuals in society.

Conclusion

As individuals and people collectively come to understand and appreciate that their personal information is ever-more transportable, frangible, fraught with risk, and, yes, valuable, behaviors, laws, social mores, and entire aspects of privacy in our society must change to reflect the new-found paradigm.

There will be growing pains in securing personal information, and we in the security field face them every day. It is our task, then, to usher in that new age with as little damage and pain as possible, in order to restructure this information-based culture as best as we can, for all involved.

Additional Resources

The Virginia Information Providers Network (VIPNet).

Hertz' corporate privacy polic..

Virginia state code pertaining to sharing driver records.

Cracking cell phone encryption.

About the author

Ben Malisow, MBA, CISSP, CISM, SANS GSEC, is a former Air Force officer and has provided security consulting services to DARPA, the FBI, and United States Department of Homeland Security/TSA. For the purposes of full disclosure pertaining to this article, he is an American Express cardholder, a frequent Hertz client, and a former resident of the state of Virginia.