A False Sense of Security

by J. David Oder

Before Sept. 11 there was very little national focus on the protection of credit card information. Some states had laws about throwing away carbons from imprinted credit card slips, but little was being done about the protection of information in the rapidly expanding electronic processing of credit cards. Most believed that the complexity of credit card processing was ample protection. Some states tried to protect cardholder information by requiring that credit card receipts not print the entire card number and expiration date. These laws helped from the occasional loss of a credit card receipt, but did nothing to protect against a major attack on the electronic payment business.

With the advent of the Internet, the problem of a major attack on the electronic payment industry made national news. It seemed almost every month there was an article about hundreds of thousands or millions of credit card numbers stolen off an unprotected Internet site. This caused a knee-jerk reaction that the Internet was not safe and we saw many TV and newspaper articles warning not to use credit cards on the Internet. One could argue that this was one nail in the coffin of the dot-bomb collapse.

Before we proceed we need to address the security of the Internet. The Internet is no more or no less secure than any other communications technology. With all the "hubbub" and commentary on the ills of security on the Internet one might ask how I can make that claim. If during the dot-com era, developers of systems on the Internet had taken the same care that professionals had long taken using leased lines and dial telecommunications, the disastrous losses of credit card information could have been avoided. Unfortunately, with the rush to make millions on the Internet, everyone that knew anything about the Internet threw systems together to get to their IPO or to get the next round of venture capital. There was only time to beat the other guys to market, not time to make sure the systems were reliable, let alone secure. With the *bomb* of the Internet, many of the people involved have left, looking for the next CB radio or cell phone scheme, and the Internet is more and more in the hands of professionals. Thus, it is becoming more and more secure.

VISA's CISP

12 steps to secure your credit card data.

These rules are basic security procedures that should be followed to protect any sensitive data.

1. Install a lock.
2. *Make sure the lock works and you keep it oiled.*
3. Close the door and lock it.
4. *Don't store your stuff in the middle of the lobby.*
5. Regularly make sure the lock hasn't been tampered with.
6. *Only give keys to people who need to get to the files.*
7. Number the keys that you hand out.
8. *Do not hand out the master key.*
9. Have a camera or access system watching who goes in and out.
10. *Regularly check to see that the door is locked.*
11. Make sure you have a list of the people who have keys and you have a set of rules for who has access to the file room.
12. *Lock the door, literally.*

With the formation of the Department of Homeland Security in the post-Sept. 11 era, Secretary Tom Ridge created a list of threats to our nation's security. Along with the obvious air travel, ports and nuclear and chemical plant security, Ridge listed protection of the nation's banking system. Within this category the credit card industry was pointed to as a possible target of terrorists that would disrupt the U.S. economy or those who looked to fund terrorist operations.

With a great deal of bad publicity and some prodding from the government, the card associations have created standards for credit card information security, which they are just now starting to enforce. Visa's Cardholder Information Security Program (CISP), MasterCard's Site Data Protection (SDP) and American Express' Data Security Operating Policies (DSOP) are all focusing on the protection of cardholder data when public networks, like the Internet, are used to process or access credit card data.

These various sets of standards do a good job defining a minimum standard that must be met to protect cardholder information. Over time, all systems which access the credit card networks will be required to meet these standards and to undergo an independent audit assuring their conformation to the standards. Visa's CISP is the most comprehensive standard including 12 rules or domains that those connected to the credit card networks must adhere to. These 12 domains are basic security procedures that should be followed to protect any sensitive data, let alone credit card data.

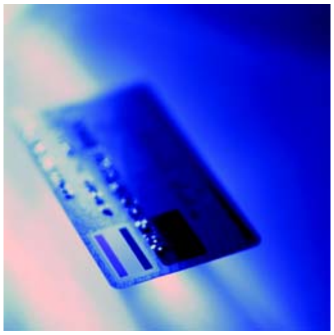
To professionals in data processing and credit card transaction processing, these rules are similar to rules you might use to lock a file room.

While these would seem like very simple rules to follow, it is amazing how many people who process credit cards on a daily basis don't follow them. To Visa's credit, CISP includes very detailed and specific processes that companies must go through to meet these CISP requirements. To have any level of security and to not find yourself on the evening news, all of your applications that process credit cards should meet and regularly go through an audit to assure adherence to these minimal requirements or should use a gateway application that is acknowledged to meet or exceed these requirements. You can find the actual requirements on Visa's Web site at http://usa.visa.com/business/merchants/cisp_index.html?ep=v_sym_cisp#b.

Visa, MasterCard and American Express have done a good job protecting cardholder information. Their 12 domains go a long way, but they are not enough to completely protect your credit card operation. Where is the protection for the merchant? Where is the Merchant Information Security Program (MISP)?

It seems that the card associations are more interested in protecting the cardholders than protecting the people that accept the cards. We would suggest adding four more domains.

1 | Build a policy and train your employees to protect against social engineering. Social engineering is basically the "con" which allows a person outside the organization to get sensitive information about your operation through subterfuge and force of personality. To learn more about this subject I would suggest reading "The Art of Deception" by Kevin D. Mitnick.



2 | Protect merchant-specific information. It is important that merchant information be protected like you would protect your checking account number and PIN. Processors, some gateways and many point-of-sale vendors are very cavalier about disclosing merchant identification numbers. For security reasons I won't disclose how these numbers could be used, but suffice it to say, a single merchant information number is worth a lot more than hundreds of credit card numbers. Make sure that you protect your merchant numbers and that the vendors you use have all four of these domains in place.

3 | Protect against employee fraud. Make sure that the systems you use don't allow employees that you have given passwords to manipulate the system for their own personal gain. Merchants lose more credit card money from inside jobs than from all the hackers that steal credit cards.

4 | Implement background checks of those who handle credit card information. Employees with criminal backgrounds or who have financial or substance abuse problems are 10 times more likely to manipulate systems or disclose merchant information for their own personal gain than those who don't have these problems. It costs less than $125 to do a drug test, a local and nationwide criminal background check and a comprehensive financial background check. When you get the results of these inquiries, use the information and don't hire people with any of these problems. You will save hundreds, thousands or even hundreds of thousands of dollars and a great deal of bad publicity.

If you, your vendors and financial institutions adhere to these four rules in addition to CISP, you should have real security. You will know that you have done what you can to protect your company and to guard against your funds financing thieves or terrorists.

We have already found out that the complexity of the credit card networks is not ample protection and any sense of security we get from that belief is wrong. The requirements of the various card associations, such as CISP, go a long way toward security, but they really only protect the cardholder's information. Every vendor you use should at least subscribe to, be audited for and be acknowledged as compliant with CISP. But without the four additional domains outlined above being adhered to by your company, your vendors and the financial institutions you use, compliance to CISP only gives a false sense of security.

J. David Oder is president/CEO of Shift4 Corporation, a Las Vegas, Nev. firm, which supplies electronic payment applications and services to hospitality merchants worldwide.