

# MCIF: Does it mean Missing Customer Information Files for you?

Tom Desot, VP of Client Services and Security Operations Digital Defense, Inc.

Just as doctors will tell you that high blood pressure is the “silent killer”, systems exist on your network that put you at risk without your knowledge. And, just like high blood pressure, everyone knows about these systems, but most people do not worry about them. That is, they do not worry until it is too late. One of the most important “silent killer” systems is typically found in the Marketing Department of many financial institutions. It is the MCIF, or Marketing Customer Information File system.

So why should you worry? Consider what happens every month in most financial institutions. At month-end, the Marketing Department will typically get a “cut” from the core processing system that contains components of the same sensitive information that is resident on that system. The MCIF system stores all of the aggregate balances of members or customers, quite often along with dates of birth, addresses and other sensitive information. This data storage allows the Marketing Department to run queries against the database and determine which members or customers are most profitable, who falls in the highly desirable 18-35 year-old range, and who needs to receive the flyer for the next IRA promotion.

If yours is like most financial institutions, your core processing, home banking, and imaging systems are treated like the crown jewels (which they are), and as such, are hardened to make breaking into them a challenge for even the most astute hacker. Regrettably, most people leave the MCIF systems to fend for themselves.

Fortunately, the steps that most organizations need to take in order to protect their MCIF systems are similar to things that they are already doing to protect their core processing and other critical systems.

## Patch Those Vulnerabilities

One of the easiest things that an organization can do to protect the MCIF system is to keep up-to-date on the latest patches for not only the operating system, but the applications that reside on the server or workstation as well. By doing so, they can eliminate many of the vulnerabilities that might allow an attacker easy access. Be wary though, as some patches might have an adverse impact on the MCIF software itself. If you are unsure about what will happen when you patch the system, check with the vendor first and ascertain if they have encountered issues of their own or have heard about problems from other clients. If they indicate that there are problems with the MCIF software after patching, make sure that you obtain a good idea of the amount of testing they are going to do before you can patch. If you consistently find that the vendor cannot provide a timeline, it may be time to look for another vendor. Remember, it is your members or customers, as well as your data, which they are putting at risk.

## Turn on the Firewall

Most servers and workstations now come with a built-in firewall that the system administrator can enable and disable. For those that do not, there are numerous commercial “after market” firewalls that can be installed and utilized on the system.

The primary reason that you want to employ a firewall on the MCIF system is to limit network access to any services that are running. For example, most MCIF systems will utilize some type of database to store the member or customer data. If the database server provides remote connectivity, you will want to be able to limit the number of systems that can potentially connect to the database and run queries against it. This is especially true if the database has been set-up without an administrator or “SA” account password.

## Limit Use of the System

The server or workstation that supports the MCIF system should be a single-use system. In other words, institution staff should not utilize the system to perform their normal day-to-day duties.

Though a single-use system may appear to be an expensive proposition at first, consider what would happen if the staff member visited a web site that compromised the MCIF system and provided an outsider with full control. Additionally, making the MCIF system operate on a dedicated server or workstation helps ensure that other software will not be loaded that may overwrite or damage critical files that the system needs to perform properly. If the MCIF system is located on a server, make sure that you are not offering web or mail services on the same server. Otherwise, having these other services on the same server provides numerous vectors of attack and places your data in harm's way.

## Use Anti-Virus Software

While it may seem like a "no brainer" now, you would be surprised at the number of systems that do not run anti-virus (AV) software. The key point to focus on, is working with the vendor that supplied the MCIF system to ensure that the AV software will not damage any of the database files that the system needs to function properly. More than likely, your vendor will have a recommended AV package that they have tested and found to work well with the MCIF system. If, after speaking to the vendor, you find that they do not have a preferred AV package, ask them if they know of any files or directories that you should avoid having the software scan. More than likely, they can point you in the right direction and ensure that the AV software works as intended.

## Use Strong Passwords

It is very important to make sure that all users utilize strong passwords on the MCIF system. This applies to the MCIF application itself, as well as to the local workstation or domain credentials that they use to access the system. For those MCIF systems that do not require their own password, a strong local user or domain password will protect the data on the system and prevent someone from gaining trivial access. Regardless, the passwords should be at least eight characters long and consist of numbers, letters and special symbols.

I spoke earlier of the database administrator password. These are just as critical as any other password, as they can provide the same level of unfettered access as a system administrator account. If you are unsure whether your MCIF system has a database or a database administrator password, check with your vendor; they should be able to provide you with information on the implementations for their product. As a side note, ask the vendor if they use a common database administrator password for all of their clients. If they do use a common password, ask if you can change the password for your system to one that is unique. This ensures that even if an attacker knows the common password, they will not gain easy access to your database.

## Encrypt That Data

Physical theft happens to organizations every day; this is a fact. Your core processing system is not that much of a concern for physical theft since the servers are typically stored in secured areas and are large enough that they would be difficult to carry out of a building undetected. However, many MCIF systems reside on small workstations in unsecured areas of the building. If a thief were to steal the workstation, they would be walking out with highly confidential information that could compromise the integrity of your organization.

If there were a high probability of theft of the MCIF system in your institution, the easiest way to provide protection would be to install the system in the same secured area as your core processing system and allow access via an encrypted, network-based technology. Unfortunately, this is not always feasible due to access needs from the Marketing Division or the unavailability of space. So what should you do? You will then need to encrypt the MCIF data stored on the hard drive.

Quite often, when people hear the word “encryption”, they see pictures of scientists and mathematicians standing at blackboards, writing out long, complex equations. As such, they think encryption is something that is going to be hard to implement and understand. Fortunately, data encryption technologies have come a long way in the last few years and have become very user friendly. Some of the newer technologies allow for the creation of encrypted containers to store your data, while others encrypt the entire disk for you. By using encryption in either fashion, you can prevent a thief from easily gaining access to the data stored on the computer he has stolen. The key here though, (and it may seem like a broken record is playing) is the diligent use of strong passwords. Whether you use an encrypted container or encrypt the whole disk, if you have a weak password assigned to the container or the system, it once again becomes trivial to gain access to the sensitive data.

Other technologies offer the use of “tokens” that access the partition or disk via a USB fob, but they typically are more expensive and harder to use and maintain. Besides, why spend more money when you can spend a little time picking a good password and then use the funds for another project?

## One Last Thing, Transmit the Data Securely

As I stated earlier in this paper, MCIF systems get a “cut” from the core processing system on a monthly basis. Most organizations will transmit this data between the two systems via the use of FTP (File Transfer Protocol) or “sneakernet” (placing the files on floppy disk or CD-ROM and walking them over to Marketing).

There is an inherent problem with both of these methods though. Let us address FTP first, because it is probably the most commonly used of the two. FTP is a service that allows one to move files back and forth between systems by uploading or downloading them from certain directories. The biggest problem with FTP is the fact that all of the data will transmit across the network in an unencrypted fashion. As such, anyone sniffing the network at the time of the transfer is going to be able to capture a great deal of interesting member or customer information.

A better approach would be to use SFTP (Secure FTP) or SCP (Secure Copy). Both are similar in nature to FTP in that they are network based and allow you to move files back and forth between systems. However, unlike FTP, they do so in an encrypted fashion by setting-up a secure tunnel (much like a VPN), between the MCIF and the core processing system before the transmission of any data. They also have the capability of using either password or public key technology for authentication.

The second method comes from the advent of “sneakernet”. For years, this was the easiest way to move data back and forth between systems. The problem in this scenario is that more often than not, people do not encrypt the data when placing it on the floppy disk or CD-ROM. As a result, someone can compromise sensitive data if the disk is lost or stolen. Using this transmission method is safe with the addition of one extra step to the process. The data needs to be encrypted using PGP or a similar technology prior to transferring it to a disk or CD. If someone in Marketing has a PGP key, the data can be encrypted with their key, or it can be placed in what is usually called a self-decrypting archive (similar to an encrypted zip file) that utilizes a very strong encryption algorithm like AES or Triple-DES and then assigned a strong pass phrase.

## Conclusion

MCIF systems are highly advantageous. They tell you who to market to and why, and they help you make critical choices about your strategic marketing plans. By taking the simple steps outlined above, they can also become a secure repository for your member or customer data and one of the many secure systems on your network.