



Am I Safe? Security Concerns in the FileMaker Workplace

If you read major news sites online, or the business section of any newspaper, you are aware that there have been some significant, high-profile breaches at major retailers like TJ Maxx and Barnes & Noble, in which 40 million credit and debit card numbers were stolen. The justice department arrested 11 members of an international ring in connection with the thefts. The full ramifications of this will probably not be known for some time.

The August 7, 2008 issue of the Los Angeles Times features an article in which a consultant named Dan Kaminsky identified what is perhaps the largest potential breach of Internet security in the last ten years. He has worked with most of the Fortune 500 companies to patch this hole before it could be exploited, but others may be slower to catch up. The problem lies in the DNS system and the way it can be hijacked by malicious sites pretending to be someone else – even where SSL certificates are used (like the kind that supposedly makes online shopping safe). Companies that sell SSL certificates have recently taken steps to verify customer identity and thus head off this sort of thing from happening.¹

A respected medical organization, UCLA Health System, recently discovered that celebrity patient records had been inappropriately and illegally viewed by, at last count, 127 employees².

These are just a few examples of the many ways that our valuable information is constantly under attack. Hackers will continue to come up with unique new ways of getting their hands on sensitive data, but it is important to keep in mind that it is easier for them to focus on the most vulnerable targets. A little common sense can go a long way.

This article is intended to give you and your organization some general information regarding security. While it is by no means definitive, it will hopefully give you some guidance on where to focus your energy in regards to security issues.

Types of Security

For purposes of this article, there are three main areas upon which you should focus when it comes to overall security: external network/firewall, internal network, and your database. All of these can be exposed to various threats.

External Networks

This is the point of entry for your network. Think of it as a front door. Just as you might prefer to keep your front door locked, your network is protected from outside intruders by a firewall, which is controlled by your router. You should consult with a reputable firm to help you properly configure your router so that it is not vulnerable to attacks.

¹ <http://www.latimes.com/technology/la-fi-hacker7-2008aug07,0,216105.story>

² <http://www.latimes.com/news/science/la-me-health5-2008aug05,0,5856834.story>

Many people, when they think about security, think of this aspect first. After all, your home is more likely to be robbed by someone from the outside, right? This may or may not be true for your home, but it is not at all the case when it comes to your office and data theft. **A significant threat, though painful to think about, comes from people you see and speak with five or more days a week. When it comes to theft of intellectual property, customer or financial records, or intentional exposure of private or sensitive information, two-thirds of cases are likely to occur from within the organization**³. Identity theft, on the other hand, is more often perpetrated by outsiders. Worms, viruses, and keystroke recorders come from outside, but are usually downloaded by people inside the organization, without their knowledge.

Internal Networks

Everyone behind your firewall is on your internal network. This includes employees, contractors, IT administrators, and management. As mentioned above, there is always a potential threat from persons such as these. It is difficult to manage a company without a free and steady flow of information. Every company is different in philosophy and resulting policy. People who feel trusted find it easier to be trustworthy, but that trust has to be well placed.

It is said, “good fences make good neighbors.” This can apply to internal network security. Reasonable boundaries within the workplace are acceptable. I cannot count how many times I have seen passwords written on post-it notes and stuck to a computer display’s edge, or have seen a manager casually share a password with an employee with a lower access level. This is tantamount to handing someone your ATM card and PIN on the assumption that they will only make deposits. Why steal sensitive information with your own account if you can use someone else’s?

Databases

Databases are designed to store information that is often, by nature, sensitive. It is always a matter of concern for us to limit exposure for our clients. In the legal sense, the word “exposure” refers to what potential liabilities you are faced with if a practice you employ goes terribly wrong. While lawsuits or even criminal action are valid concerns when thinking about this, what you have to lose, at the very least, is the lifeblood of your business: your customers. It’s certainly safe to say that you do not want to have to make the phone call in which you inform your valued customer that her credit card number has been stolen – along with that of hundreds of others as well. While it is sometimes necessary to store such information, you should take proper measures to protect it with encryption, password protection, access auditing, and other reasonable measures.

You may be wondering, at this point, just how safe your database really is. First of all, it is important to mention that The Alchemy Group always gives this question plenty of consideration when deploying a system. We use several industry-standard methods to maximize security. We use external authentication to allow user accounts to be managed outside of the database structure. This allows for passwords to be stored in such a way that they cannot be obtained by hacking into the database in some way. They simply aren’t stored there, but are instead within a well-secured, industry-standard repository on the server.

We always recommend that database files are not available to users through any shared volume over the network. This keeps them out of the hands of all but system administrators, while FileMaker’s network sharing scheme still makes the data available to those who are authorized to see it.

³ CSO Magazine eCrime Survey, September, 2006

FileMaker Server offers very strong security, and we follow industry best practices to ensure that your database is not exposed to prying eyes. Nevertheless, there are additional measures to be taken when the information has a higher degree of sensitivity. For example, if you work with patients, we follow HIPAA regulations to safeguard their data. If you store credit card numbers, we follow the guidelines enforced by major credit card processing gateways like Authorize.net, including encryption of credit card numbers. We also take steps to make sure such information is not available onscreen to users who should not have it.

Backups

No discussion of security is complete until disaster preparedness has entered into it. After all, you are the custodian for important data for your customers, data that may be compiled in a unique way. Should it become unrecoverable, you have lost not only the lifeblood of your company, but perhaps theirs as well.

Fire, water damage, and theft are the first things we all think of when someone says the words, “disaster recovery.” Far more common, however, are loss due to accidental or malicious user actions, and loss due to corruption. Fortunately, FileMaker offers useful tools for protecting and backing up your data. We always make sure our clients have a clear and working backup policy, and we can work with you to devise one that best suits your needs, including onsite backups, offsite storage and retrieval services, and other long-term archiving methods.

The Alchemy Group is Here to Help

Every security situation is different. Depending on your business model, type of information collected, and company profile, security may be your first thought, or it may rarely cross your mind. Regardless, you should always have a security plan, and **we are, of course, [always here to help](#).**

Best Regards,

Bob Shockey, President
Alchemy Consulting Group, LLC

P.S. The Alchemy Group has a few limited spaces coming open in our project schedule to support new clients. Please feel free to forward this article to colleagues who might find it useful – and, as always, we thank YOU for sharing.