ArcSYS, Inc.– Draper, Utah

Volume 16, Number 7

July 1, 2015

ArcBITS Newsletter

Inside this issue:

Castles and Pirates

How secure is the data on your computer system? Every day we are saturated with yet another news story of a breach of data. You would think that giant retailers like Target could protect their data. Or, better yet, that the U.S. Government would have adequate safeguards in place.

1000 years ago the nobility protected themselves by living in stone castles surrounded by moats. Assailants became quite clever and perfected the art of catapults and would launch huge boulders or flaming pitch to pass over the castle walls. What was the solution? Build taller walls and move the moats further from the castle. Finally, the assailants figured out one thing that was nearly unstoppable: Tunnels. It was certainly impervious to arrows and boiling oil from the ramparts. Not only that, the reverberation of constant pounding was relentless and drove the castle dwellers nuts. Once inside, the assailants showed little mercy.

Until 250 years ago there was no reliable way of measuring longitude (east-west), only latitude (north-south). Merchant ships knew this. Pirates knew this, too. If you were a pirate, all that you had to know was the latitude of, say, Lisbon Portugal. You'd park your ship on this latitude and eventually you'd find a merchant ship homing in (dead reckoning) on this latitude, too. Score.

Strategies haven't changed much over the centuries. We add more firewalls. We change our passwords. We fill out endless checklists telling ourselves that we and our business associates are HIPAA compliant. If you're a hacker, it doesn't take much rocket science to know which hill the Target castle is atop. (Your IP address is your latitude/longitude.) Then, it doesn't take long before they can dig underground by trying variations of user names and passwords. If they are successful, it doesn't take long before they can clean the castle by stripping files.

If you're a tiny castle, the marauders may skip past you while looking for bigger treasure. But when the big castles have been cleansed, they'll come back looking for their next pickings: Insurance. Hospital chains. You get the idea.

And, just when you think you've escaped all external perils, we now face the biggest threat: A disgruntled employee. Sadly we've seen an airplane pilot and a co-pilot go rogue plummeting their planes and passengers to death and destruction.

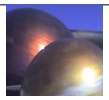
What can you do? Don't be complacent. Don't think your precautions are fail-proof. Don't leave a key under the doormat. Check all the doors and windows before you go to bed. Keep your server in a locked room. Hire the best people Sleep with one eye open. Trust, but verify. Happy dreams!

ArcSys Hot Tip

Hmm...

3 MONTHS LEFT UNTIL ICD-10 CUT-OVER!!

Although the new regulations for handling ICD-10 allow for 12 diagnosis codes for each cpt, only 8 can be transmitted electronically. Your charge entry screen can be easily expanded to handle as many codes (up to 12) as you think are necessary.



Data at Rest

One of the requirements of HIPAA is that data at rest be encrypted. What does this mean? The HIPAA Security Rule *is not specific* about the exact set of best practices and tools to protect data at rest. The concern focuses primarily on a set of computer files that are no longer in the control of the business. This means things like laptops, smart phones and external disk drives.

Red Planet does not store patient data on pcs, laptops or smart phones. To that extent, you are compliant. However, that doesn't stop someone from taking pictures with a smart phone or screen dumps of patient information and storing that in files. You can only define a business policy saying that you don't.

As you know, the Windows world is made of applications (the modern Tunneling tool) and files. If you have a .pdf file, you can read it with Adobe. If you have .jpg file, you can see it with Windows Viewer. Try to open a .pdf file with Excel, and it won't work. If you try to change the extension of a file from .xlsx to .pdf and then open it with Adobe, it won't work. If you were able to "view" the raw file that defines a spreadsheet, for instance, it looks like gibberish. The same for a .pdf file. But, when paired with the right program, gibberish becomes rows and cells.

Red Planet is similar—but a little different—because of its use of Mvbase and Wintegrate. Mvbase is a data base tool. If you were to look at the raw file, you'd see zillions of numbers that, when *managed* by Mvbase, combine disparate information into files and records. In order to see this information, we employ Wintegrate to display the data. Thus you need three things to access your Red Planet information: Data file, Wintegrate, Mvbase. The latter two are licensed products (means $$$) and are not easily obtainable.

So let's say our sneaky pirate down the street is able to finagle a copy of those two products, the next task is to get the data file. How? Send a mole into your organization under the guise of being an auditor from an insurance company. Send a repairman to look at your Internet modems. The data file itself is not accessible from a workstation (unless you've shared the backup folder with all the workstations). The data file is not accessible from the Internet, either, because of the Mvbase methodology. So our mole has to physically get to the server. And, if they are able to get to it and you don't have the password to Administrator sitting on a Post-It note, then you are pretty safe.

As you can see, there are enough precautions in place that your patient information is "relatively" safe. If you take enough precautions and build your walls high enough and move your moats far from the castle, your marauder will go in search of easier pickings. (But, then the Target IT people thought they were secure, too.)

If you backup your system to a flash drive or external disk drive and take it off site, then an accidental loss increases your exposure markedly. You *must* utilize a Windows encrypting tool to hide the data (see first paragraph). If you are using Carbonite, MozyPro or some other offsite backup service, those files are encrypted. Again, don't publish your user name and password to gain access to those files with another Post-It note on your desktop.

Last, but not least, Red Planet has controls to limit the access of looking at information and updating data by employees as well as business associates. This requires the system manager *to take the time* to set up who has access to what. When employees leave, their user name needs to be deleted. When a messages appear about illegal logon attempts, they need to be investigated. When an employee with remote access by way of Wintegrate leaves, that product (a Tunneler) needs to be de-installed. Red Planet has tools to hide data from being examined by clever employees, too. Starting July 1, all employees will be required to change their passwords. We recognize it is a hassle, but it is necessary and important.

We're watching out for you, too. Our ethics and business principles respect your patient information.