West Texas Cyber Security Consortium

Security for the Real World – Password Policies

Posted on January 13th, 2014 by Ron Woerner

Passwords suck. They always have; they always will. But we're stuck with them. They are the cheapest and easiest means of user authentication.

With passwords, come the ubiquitous password policies. This post addresses two of them seen at most organizations*:

1. Thou shalt not share they password.
2. Thou shalt not write down thy password.

* "Thou shalt" isn't usually used in policies. I'm using it for effect.

There are many problems with these rules. First, they are almost impossible to enforce, unless it's a really small organization or you have a large police force. Second, they are often violated by the top echelon in the company. How many CEO's share their account with their admin? Are you going to tell the CEO that he's violating the company policy? That's a CLM (Career Limiting Move) if you ask me.

Rules like the ones above are to protect the organization, not the employee. They cannot be enforced, except when something bad happens. Then, the enforcer can point to the policy and report the violation. I call it a "speed limit" policy, which are good to follow, but aren't continually nor consistently enforced.

Here's the key to making those policies work: ***make the user responsible for his/her account***. The policy statement would then be, "All users are responsible for protecting their login credentials from unauthorized access like they would protect any other corporate asset." This puts the onus on the user. If someone gains unauthorized access to the user's account because he/she didn't follow the rules, then the user is accountable. They are guilty until they can prove themselves innocent. If someone (like the CEO) wants to share their account, they can as long as they realize that's it's them who will be held responsible for any actions taken by the other party.

With so many passwords to remember, people need to write them down. Telling people not to just isn't realistic. Some use a password vault application. Others use a piece of paper. Both are fine as long as it's rigorously protected. It's fine for people to write down their passwords as long as they

store it in a very safe location. My mom has a piece of paper with all of her passwords on it in a desk drawer in her apartment. I'm fine with it, since I may need it one day as her power of attorney. Her apartment is in a secure facility, so the risk is minimal. There's a lot bigger risk of her becoming incapacitated and me not having access to her accounts.

That's what it comes down to: understanding RISK and establishing Accountability. What are the risks associated with the actions? Who's responsible? Answer those and you make a cognitive decision that's both realistic and enforceable.

http://blogs.bellevue.edu/cybersecurity/index.php/category/online-safety-tips/