The Safeguard
In a recent study related to GLBA Risk Assessments, we found that 47 of 207 different vulnerabilities (about 23%) could be substantially mitigated with the use of Strong Passwords. Though non-inclusive, this article can steer you in the right direction towards strengthening your first line of defense, your number one mitigating control: the Strong Password!

What is a Strong Password?
Experts debate the definition of a strong password, but the approach we recommend includes six factors. Preaching "the six factors" will ensure better user comprehension. As such, a Strong Password utilizes:
1) Upper case letters
2) Lower case letters
3) Special characters (such as: !, @, #, $, %, ^)
4) Numbers
5) No dictionary words
6) At least eight characters long

An additional requirement by the FFIEC is "time before enforced change" as a control. Some banks require as long as 90 days, while others require as short as 30 days. There are good points on both sides of this debate. With our approach, the stronger your passwords, the less you have to change them. If your employees all use strong passwords, 90 days presents little risk. If not, the risk of weak passwords must be mitigated with more frequent changes. This can be used as a motivating factor during your Password Campaign!

The Password Campaign!
We encourage our clients to use a coordinated process that involves three key approaches:
• Policy   • Awareness/Motivation/Empowerment   • Password Management

1) Policy: Two types of password policies include a User-level Policy, usually communicated in a wider-reaching Acceptable Use Policy (AUP); and a Technical-level Password Management Procedure, which documents issues ranging from handling administrator passwords to system configuration to facilitating the User-level Policy. Here, we are primarily concerned with the User-level Password Policy.

First, we recommend the AUP include the following language under the heading, "User Accountability": *You are responsible for all activity that takes place on the Information System and the Network using your user name. If the security of your user login is compromised, you are still responsible and liable for all activity under that user name. Thus, you must learn and take very seriously all issues related to security (such as password practices).*

Next, your user-level password policy should establish the definition of a strong password, but it should also reflect REALITY. Given that the average teller has to remember 19 different passwords, your policy should separate "critical passwords" from "non-critical" passwords. Most banks consider the Network Login Password and the Core Processor Password as critical passwords. Other critical passwords may apply to specific users. Thus the AUP may include language such as "other passwords as established by your job description." Examples of those other passwords include the Fedline password, the AML database, Accounting Application passwords, Administrator passwords, etc.

Finally, the <u>User-Level Policy</u> should also include, at a minimum, the following password guidelines:
- Passwords must be unique. No using your critical password for any other applications or vice versa.
- Nobody can know your password but you, as you are responsible for all activity on your account.
- Passwords should NOT be written down.
- The utilization of the "six factors" method (see above) is required.
- Users should change their password manually if they suspect somebody knows their password. State who can show the user how to initiate a password change.
- How temporary passwords will be issued (for new employees or when passwords are forgotten).
- Critical passwords should have nothing to do with the users or other passwords (not be part of a theme).
- In addition, state how often the system will require password changes.
- It's okay to use the same password for several <u>noncritical</u> systems, or a theme for those systems.
- Critical passwords should never be memorized in your browser. Lower-level passwords may be memorized in your browser because you are using a strong network password. *Note: Some banks prohibit the use of browser-memorized passwords altogether. Our position is that if a strong password is used for the Network/Windows login, the risk of browser compromise is primarily based on a physical breach, and the user will have time to change non-critical passwords stored in the browser.*

2) Awareness, Motivation and Empowerment: Management should consider implementing a professionally designed User Awareness Training program to substantially mitigate GLBA risk. If there is strong knowledge at the bank regarding Information Security Best Practices, or if the bank has a dedicated Information Security Officer, it may make sense to develop your own User Awareness Training program. But keep in mind the value of an outside "expert" providing information that, when espoused by internal IT staff, does have credibility.

User Awareness Training should be centered around the <u>Acceptable Use Policy</u>. Though the policy covers far more than passwords, a good training session will stress the issue of passwords. Related to passwords, User Awareness Training should accomplish three primary goals:

1. **Awareness:** Expose users to statistics such as the likelihood that a security event is initiated on the internal network (64.64% according to May 2005 CSI/FBI Survey), how a security breach usually works (gain access to the network, guess password, log into somebody's account, steal information), and how passwords are the first line of defense. Be sure to explain what cracker software is and the difference in the time it takes to guess weak passwords (about 1 to 3 minutes) and strong passwords (about 3 to 5 days). Bring auditing information (see Password Management Process below) into the training.

2. **Motivation:** Stress the role users play in defending their customer's information. Appealing to the average user's desire to do the right thing, especially for their customers, is all it usually takes. Helping users see the connection between protecting their password and protecting their customers' identity motivates them to learn good password habits. Acknowledge the inconvenience of passwords, then show how it's an inconvenience worth accepting. Comparing passwords to other security inconveniences such as airport security etc. helps gain that acceptance. Stress that Information Security is not a technical issue, explaining how the world's most expensive firewall won't prevent a user from using a weak password. Build up to the fact that since we all have to use strong passwords anyway, let's make it fun and take advantage of our opportunity to practice "secret creativity." Don't be afraid to explain that if we can go with stronger passwords, we can go longer periods of time in between changing passwords. Acknowledge the irony in requiring strong passwords that you can't write down!

3. **Empowerment:** Once users are motivated to try to learn good password habits, the Awareness Training should then focus on tricks users can use to establish good password habits.

   a. <u>Mnemonics</u>: Teach your users how to replace letters with symbols and numbers and use sentences as the basis of their password. A lot of times, all this takes is showing examples such as the following:
   * P1zz@_1s_t@sty*   (Pizza is tasty.)
   * 1Tmwivb!   (I think my wife is very beautiful!)
   * mD3t@0fb*   (My dog eats toast and oatmeal for breakfast.)
   * Y1cmdp@tri!   (Yesterday I changed my darn password and then remembered it!)
   * 1@itCRatb   (I am in the Conference Room at the bank.)
   * dtC0t3cf?   (Did the chicken or the egg come first?)

   b. <u>Memory Tricks</u>**:** Once you teach users how to create a strong password, share with them tricks for remembering them:
   * Don't even bother remembering those "once-in-a-while" passwords or non-critical passwords that you are memorizing with your browser (assuming your password policy allows this.) If you forget your Orbitz password because you got a new computer since the last time you planned a trip, no problem, Orbitz will help you set up a new password.
   * Never change a password on a Friday. Most programs, as well as Windows and Novell networks, allow grace logins before you actually have to change a password (your IT people can configure this in other ways as well, so talk to them). If you're asked to change a password on Friday morning, try to get through the grace logins so that you can change it on Monday morning.
   * While making up your password, look around you and try to center your password around something that you see. Many times it may be hard to remember a password, but you can remember what you looked at while making up your password, and then the password comes to you!
   * Remember, don't write your password down! If you do, shred the paper once you're done creating your password.
   * Visualize your password as you make it up.
   * Once you reset your password, immediately log out and log back in.
   * 20 minutes or so after you reset your password, log out and log back in.
   * Don't worry if you do forget your password. The help desk is used to this and everybody has forgotten a password once or twice!

   c. <u>Password Themes</u>: Password Themes are a great way to remember several passwords that you use. The point is to help your users develop a "method" for simplifying the multitude of passwords they need to remember. Remind them that critical passwords should be unique and have nothing to do with the user or other passwords. But for the non-critical passwords, themes can be used to help the user remember those passwords. Thus, a typical password scenario would look metaphorically like this:
      * Windows Password: A
      * Core Processor Password: B
      * All other passwords: C1, C2, C3, C4, C5

Then share with the user a typical password theme, being careful to show them how critical passwords should be unique and not related to a theme:

- Critical Passwords:
    - G0ing_2da^S@!   Windows Login Password (Going to the USA)
    - 1n_M1_d3$k!   Core Processor Password (In my desk)
- Non-critical Application Passwords:
    - mD1@bgS*   My dog is a big German Shepherd.
    - m!bTd%t!   My little Boston Terrier does great tricks!
    - mDc^1tY!   My dogs chase rabbits in the yard!

3) Password Management: As described above, a good password control process also involves good Password Management Procedures. These are technical-level procedures that includes activities and controls such as proper configuration so that strong passwords are required by the system at least at the network level, methods of auditing passwords (see Password File Analysis and Report below), and how management will respond in the event that passwords are not being used properly. It also includes proper documentation and archival of "shared administrator passwords" such as your web hosting password, the administrator passwords to your network and applications, your domain registrar password, etc. The primary consideration here is the use of good auditing processes to ensure enforcement and awareness at the user-level.

Password File Analysis: This policy compliance audit method, commonly known as "password cracking," uses software that "any twelve-year-old kid can download off the Internet for free" to guess your passwords. The purpose of this process is to demonstrate the power (in terms of time gained) of strong passwords as well as measure the enforcement of the bank's existing password policy. The most common software used for password file analysis is l0ft Crack, John the Ripper, and Cain and Able. Expect to spend about $650 or so for a licensed copy of the cracker software, though some freeware versions are available. Consider the value of hiring a third party to conduct password file analyses because of the credibility and "wow impact" of showing in your Security Awareness Training the % of passwords gained in less than one minute by an outsider.

Reduce Your Risk!!
Whether you have your internal staff implement a password file analysis or outsource it, the point is to bring metrics into your Security Awareness Training that helps your team understand the important role they play in securing your information system. No matter how you view it, passwords are your first line of defense against security breaches. A coordinated Password Campaign will substantially reduce the risk your bank faces!

About the Author: Dan Hadaway, CISA, CISM
Dan has worked extensively with banks on policy issues, engaging on projects ranging from gap analysis to developing a full policy set for denovo banks. He can tailor his consulting to any size bank, working on simple user-level policies with banks as small as one location to overseeing the entire IT strategy for a publicly held company. He has provided management-level regulatory compliance training for Fortune 500 companies as well as user-level awareness training for the smallest of banks. His strength is helping banks decide where in the "security/compliance spectrum" they should be. He has helped develop risk management programs and processes for banks as large as 2.5 billion and as small as 26 million in assets.

*He is the Managing Partner of **infotex**, an Indiana Bankers Association Preferred Service Provider in several areas, including Information Security Training.*