

Sometimes Say 'Never': An IT Manifesto

Shhh! I am huddled over my laptop, furtively glancing both ways

It's not that I have violated any laws, though I have been thinking lately about Moore's Law. And no, I have not been unethical. But I have decided to risk my relationship with some auditors and examiners in order to put forth a proposal.

You see, I am auditing a bank that requires all employees to change passwords on the network every 30 days. Yes, 30 days! Plus, they have been charged by a zealous examiner to require customers to change online banking passwords every 60 days. Customers!

As a certified information systems auditor facing inner conflict over the recommendations I am occasionally compelled to give to my clients, I have learned to use the following statement: "With careful enforcement of mitigating controls, you can justify a 90-day password expiration requirement."

I suggest that if you have controls in place to enforce strong passwords, then the risk profile changes. Let us clarify that I'm referring primarily to the front line of defense: that network password that you must have in order to gain access to confidential information, some of which has second and third layers of password protection.

Even though Microsoft does not allow us to automatically enforce appropriate strong password guidelines for network logins, strong passwords can be enforced. And though Microsoft continues to confound users with the "choose three of four" routine, and doesn't offer a dictionary checker, strong password controls can still be implemented.

I submit that strong awareness training can overcome this Microsoft vulnerability. Let me define "strong awareness training" as a process which includes a periodic password file analysis and feedback routine. Cracker software is run against the network's password file periodically, and any employee whose password is guessed in less than a "threshold time" gets to change his or her password. The routine should be performed every quarter, with the threshold set at the time you think your network team (or intrusion detection provider) needs to detect and respond to a cracker incident. For our clients, we recommend a four-hour threshold.

As part of our company's audit process, we perform the password file analysis. We provide several metrics from the analysis, including how many passwords can be cracked in less than two minutes, an hour and the four-hour threshold time. We praise banks for increasing the number of passwords "not cracked," given a two-day shut-off.

It is easy to learn to do your own password file analysis. The banks that do their own periodic password file analysis and give feedback directly to users have the highest success rate.

Which brings me to Moore's Law: according to which, by the year 2019, computers will be 32 times faster than now. We think this means that password strength requirements will soon increase to nine characters from the eight we're currently using, because as the computers get faster, the cracker software gets faster. Speaking of which ...

Hercules Has 6_F2ct0r\$

My associates and I have attacked hundreds of password files and have found that a windows password with the following six factors will last at least four hours under the cracker software, often past the two-day shut-down of our analysis:

1. At least nine characters (used to be eight, but software and computers are getting faster);
2. Upper-case letters;
3. Lower-case letters;
4. Numbers;
5. Special characters;
6. No dictionary words.

Number 6 is critical. The cracker software can get through a dictionary in 20 seconds. So a password like America#1, with five of the six factors, is really only a three-character password, and can be guessed in less than an hour ... perhaps in less than two minutes if the cracker software is run on a fast computer.

There are other important elements of most password policies that can be vexing:

- Passwords must be unique to each application;
- Do not give passwords out to anybody;
- Do not write passwords down;
- Change passwords every [fill-in-the-blank] days.

The Numbers N1N3+ee/

I read a study not long ago that concluded that the average teller has to remember 19 different passwords. Partly out of that disbelief—and mostly because I can't remember where I read the study—I have taken to counting how many passwords a teller has to remember when I work with my clients. It turns out that 19 is on the low end.

Picture a teller coming into the bank in the morning. First he or she logs into the network, then into the teller systems. Before long, the teller will need to log into the time-tracker program to look up a record that requires logging into the imaging system. Sometimes a teller needs to log into the loan inquiry application, and certain institutions require tellers to log into the STAR system or its equivalent.

Next comes the password for the online signature application, then the portal for looking up vacation time, as well as checking out the precious few healthcare benefits banks can afford after purchasing all these applications. Factor in the voicemail password, and by mid-morning we're already up to nine different passwords for the teller to mentally retrieve.

But wait, there's more. Let's add the password that Tilly the Teller uses to log into her home computer, her online banking account, her personal e-mail account, her other personal e-mail account and her ATM pin. If she's youthful, add in the myspace.com, facebook.com and youtube.com passwords. Don't forget other social sites and cell phone voicemail. Now we've hit 19. Not to mention amazon.com, itunes.com and Tilly's personal blog.

We Have the Core Pa\$\$^^ord!

We auditors and some examiners have taken to training people on the use of what we call the “core password.” The person who introduced this concept to me is a good friend and client, Larry Turner, chief information officer of First Bank Richmond, NA. Many years ago, Larry showed me how the teller can reduce the mandatory number of passwords to just a handful.

The key is using a good, strong password in all nine of your business passwords, and a different one for all 10 to 12 of your personal passwords. You start with a strong password, i.e., the core of your passwords. For the sake of this manifesto, let’s use the following as our core: Manifesto --> M@n1f_st0

Then you use descriptors before or after the password to help you remember what it’s for. In our teller’s example:

- network-M@n1f_st0
- core-M@n1f_st0
- time-M@n1f_st0
- loan-M@n1f_st0
- image-M@n1f_st0
- STAR-M@n1f_st0
- sig-M@n1f_st0
- portal-M@n1f_st0
- voice-M@n1f_st0

Of course, because of technical difficulties, it doesn’t always look like the above list. Some core processors do not allow the six factors. But that’s okay, because we want the core to be separate from the rest of the password theme, anyway. So we end up with something that looks more like this:

- network-M@n1f_st0
- Upperlower1 (for your core processor)
- time-M@n1f_st0
- loan-M@n1f_st0
- image-M@n1f_st0
- STAR-M@n1f_st0
- sig-M@n1f_st0
- portal-M@n1f_st0
- 2334 (for your voicemail)

Yes, that voicemail code stands for Michael Jordan, Walter Payton, which dates me and illustrates a bad practice, because you shouldn’t use predictable numbers.

Now the teller has only three passwords to remember: the core, the teller system and the voicemail.

The descriptor scheme could be flipped for non-business passwords, but the “core password” should be different as well. It could be based on the first letters of a sentence, such as, “I use a different core password at home.” Something like: 1U@dcp2h

Then we have:

- 1U@dcp2h_home
- 1U@dcp2h_online
- 1U@dcp2h_hotmail
- 1U@dcp2h_yahoo
- 1U@dcp2h_quicken
- 1U@dcp2h_my
- 1U@dcp2h_fb
- 1U@dcp2h_youtube
- 22334

... and we're done.

“What about amazon and itunes and such?” you may be wondering. Well, unless Tilly shops there a lot, I suggest she use the “forgot-your-password-feature” right under the yellow button on the sign-in page. And Tilly’s voice mail on her cell phone? That has the number: 22334.

So we're down to five passwords then ... one handful, just as Larry promised. The network, the teller system, the core password for everything else at work, the core password for everything at home, and the voice mail number Tilly is using at home and at work.

Note that technically it is cheating a bit to use a voice mail code for home that is similar to the one for work. However our mission is to minimize risk. What is the risk that somebody would try to hack into the bank using your teller’s voice mail code?

Risk m@N&G3M%/VT: Part 1

Because of Murphy’s Law—not to be confused with Moore’s Law—the risk profile related to password expirations has changed. As a banker, you know that when we consider risk, we’re really considering the likelihood of something happening in combination with the impact or cost of it happening. Risk mitigation is often a balancing act, where we must choose between two or more competing controls. Sometimes implementation of one control may lessen the effectiveness of another control. In this balancing act, we often have to weigh the cost of two different actions against the corresponding risk of those actions.

A Short History L3\$\$0N

When people complain about a control, especially an information technology control, it is important to remember why it exists. What risk is the control designed to mitigate?

In the case of passwords, Dr. Eugene H. Spafford, director of Purdue University’s Center for Excellence and Research on Information Assurance and Security, offers the following explanation on his blog:

“Back in the days when people were using mainframes without networking, the biggest uncontrolled authentication concern was cracking ... Some DoD* contractors did some back-of-the-envelope calculation about how long it would take to run through all the possible passwords using their mainframe, and the result was several months. So, they (somewhat reasonably) set a password change period of 1 month as a means to defeat systematic cracking attempts. This was then enshrined in policy, which got published, and largely accepted by others over the years. As time went on, auditors began to

look for this and ended up building it into their 'best practice' that they expected. It also got written into several lists of security recommendations."

So the invention of password expiration is not that somebody would be able to eventually guess your password. The risk that the control was invented to mitigate is that cracker software could be used to guess your password prior to the expiration.

Thanks to Moore's Law, computers are faster, cracker software is improved, and crack attacks can guess strong passwords in as little as four hours. Of course, nowadays we also have good network monitoring systems in place, so four hours should be adequate.

Let me disclose a few other vulnerabilities supposedly mitigated by the expiration control. The longer a password remains a password, the greater the chance it will be found written down somewhere. It also is likelier to have been given to somebody "in a bind," then later neglected to be changed to a new password. This concern arises from the scenario that one day you stay home sick, and the office calls needing some information. So you ignore policy and proceed to tell your password over the phone ...

But wait. We can't even guess our own passwords nowadays, which is why the forgot-your-password feature is as much a part of everyday life as the search-box.

Risk M@N@G3M3NT: Part 2

Dr. Spafford also has written, "'Best practice' is intended as a default policy for those who don't have the necessary data or training to do a reasonable risk assessment." The password expiration control is in all our policies, because it was deemed long ago to be a best practice. The risk this control mitigates is now very low, because the likelihood factor is lowered by the strong password, which was developed to combat against cracker software.

Meanwhile cracker software is outpacing the expiration time, and risk mitigation should be viewed in terms of the cost. The need for this manifesto becomes clear when we explore the cost of the password expiration control:

- Support costs. Password expiration requires measurable resources to implement—far more resources than strong awareness training, which mitigates much more risk.
- Weak passwords. By requiring even a 90-day expiration, we inspire people to use weak passwords, when instead we should encourage use of strong passwords, which actually do mitigate risk. Our use of weak passwords substantially increases the likelihood of an authentication breach during an attack, because we decrease the guess time from days to minutes.
- Written passwords. Password expiration increases the likelihood people will write down their password. At a minimum, we resort to writing passwords while inventing new ones to satisfy the expiration process. The likelihood of a person finding a written password is far greater than the likelihood of guessing a password.

The M@N1F3\$To!

The bottom line: I am proposing that we not just extend password expiration requirements to the current "reasonable time period" of 90 days. (I am again crouching over my laptop, looking both ways.) I am declaring that, in the right circumstances, a bank should be able rise above this oppression, stand up to auditors like me, and extend their password expiration requirement to "never."

WAIT! Before lightning strikes me, let me state the circumstances:

- On the network login for starters;
- Strong awareness training.

Network—because we can easily implement strong awareness training there. It's easy to set up the cracker software against the SAM file. We eventually can do it on other applications, but let's start with the network. It is the front line of defense, where strong passwords are critical.

Strong awareness training—because this is really where you do force the password change. The new policy becomes: "If you use strong passwords, you do not have to change them. If we guess it below the threshold time, you need to change it immediately."

This change in philosophy will, in my opinion, lead to widespread use of stronger passwords. A revolution will occur in information audit exit meetings throughout the world. Bankers will like their IT auditors again. (Okay, that may be stretching it a bit!)

But seriously, the result: The strong password will eliminate the risk the password expiration was supposed to address.

Meantime, in case I hurt any feelings, maybe I'd better go talk to those auditors and examiners!

¹Department of Defense

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.