



Pivot Point Security  
957 Route 33  
Suite 111  
Hamilton Square, NJ 08690  
(609) 890-1131  
[www.pivotpointsecurity.com](http://www.pivotpointsecurity.com)



## When a best practice isn't best for your organization

by [John Verry](#) | [More from John Verry](#) | Published: 1/8/03

Category: Technology | Audience: IT Consultant

Rating: **3.8** (out of 5) [Rate it](#) Comments: 19 | **0 NEW** | [View all](#)

### Takeaway:

After a consultant performed a security assessment for a client, he was rehired a few months later to examine his client's progress. Here's what he found when he took a look at the client's approach to passwords and the corrections he had to make.

---

Several months after a security audit, a client re-engaged my firm, [COUR IT](#), to review the planned responses to a number of the audit's findings. One of the recommendations that came out of our audit was that the company institute a formal password policy. But when the client showed us the policy, we thought it might be too restrictive (at least at the time). I'll show you how we worked to balance the client's security needs with the practicality of the solution that they had proposed.

### When best practice isn't

The client's board had assigned the responsibility of addressing this particular finding to a member of the IT steering committee, which had little practical IT experience. As a consequence of the security audit, the board had moved the responsibility of creating the password policy outside the IT department. (The board argued that if the IT department were capable of implementing a formal password policy, the finding would have never been made during the security audit.)

The policy (and supporting guidelines) that the steering committee member presented to us was extremely thorough and contained all the hallmarks of a policy consistent with a current "best practice." **Figure A** gives a rundown of the policy's highlights.

**Figure A**

Attribute	Requirement
Length	>=8 characters
Complexity	Mix of alpha, numeric and non-alphanumeric (e.g., !, #, @)
Format	Mix of upper and lower cases
Password age	Passwords must be changed every 90 days.
System usage	Passwords must be different for all systems or applications.
Password history	Passwords can not be re-used for a period of two years.

Common usage	Passwords cannot be found in either Webster's Dictionary or the King James Bible.
Personal information	Passwords cannot be based on users' or family members' names, birthdays, social security numbers, or other easily obtainable information.

Client's password policy

The five-page policy included an extensive list of guidelines regarding strong password construction and myriad other issues. And although the client was clearly proud of his efforts, the knowledge he had gained, and the resulting policy, we thought that it wasn't exactly the correct fit for them at the time.

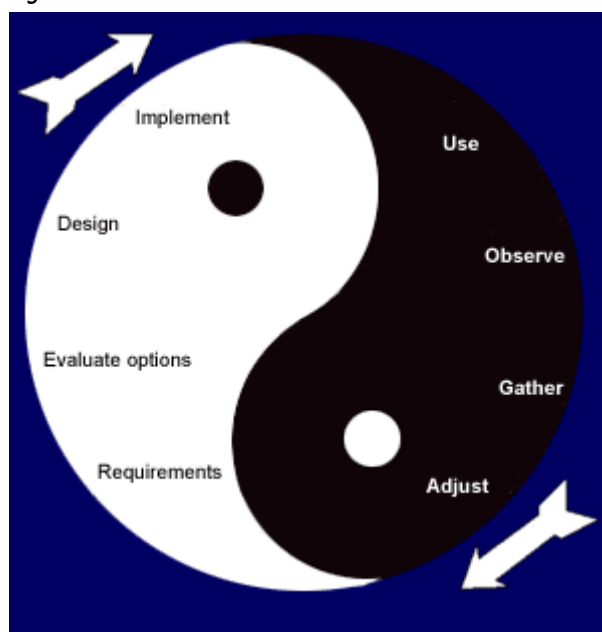
So this was our quandary: How to tell the client the proposed policy might not be appropriate at that point? Essentially, what do you do when best practice isn't?

### Chinese philosophy meets IT security

One common bond I shared with our client was an appreciation for Chinese philosophy. Previously, we had briefly discussed the concept of Yin-Yang, a foundational element of Chinese philosophy's belief in dualism, a state in which the universe is seemingly divided into two opposing but equal forces. Essential to the understanding and application of Yin-Yang is that they attempt to hold each other in balance, exerting mutual control, and that instability is the result of the two unbalanced elements.

This concept is highly applicable to the field of IT security, as shown in **Figure B**, where balance is essential and the continual flow (Yin to Yang, Yang to Yin) perfectly models its optimal iterative process.

Figure B



I've annotated the Yin-Yang symbol to show how it relates to traditional System Development Lifecycle Methodology (SDLC) mechanisms that we use to model security for key systems. I hoped that discussing the issue in these terms might be a tactful and political way to broach our concerns regarding the client's proposed policy.

### Applying and communicating Yin-Yang to passwords

Typically, when end users are forced to use complex passwords that change more frequently than they're accustomed to (or are capable of handling), they'll write the passwords down. Standard practice for many security auditors is to visit a number of workspaces and look in the typical locations (under the keyboard, yellow sticky on monitor, front or back page of prominent desktop book, whiteboard) where users often record passwords.

A lack of balance—too restrictive a policy—forces a compensatory action—writing down the passwords—which produces a result that is opposite to the one anticipated: The organizational security is reduced rather than improved.

We told the client that, based on our experiences with similar organizations, this policy might be too restrictive (Yin) for his organization, and the result of implementing this policy would actually be reduced security (the lack of balance would cause Yang to compensate). He immediately understood my concern and asked, "How would Yang compensate?"

### Balance yields reasonable and appropriate security

We argued that suddenly shifting from a policy under which individuals were using the same three character password—often as simple as "abc" or "123"—for all systems and applications, to one with which they would need new, highly complex passwords for each system every 90 days would create far more short-term problems than it solved.

For example, calls to the organization help desk (which was already understaffed) would have likely quintupled immediately. End users would have been prevented from working while waiting for their passwords to be reset. Eventually, many end users would have violated the new policy by writing the passwords down and storing them in an easily compromised place.

If the client's business requirements truly dictated the immediate implementation of his initial restrictive policies, we would have implemented additional mechanisms to provide the necessary (Yang) balance. These may have included: significant levels of end user education and security awareness training, system-level tools to enforce policy, and additional control mechanisms, such as password auditing.

After considerable discussion, we jointly revised the new password policy to simplify the requirements for the initial rollout.

**Figure C**

Attribute	Requirement
Length	Reduced from $\geq 8$ characters to $\geq 6$ characters
Complexity	Removed requirement to include non-alphanumeric characters in password
Format	Removed requirement for mix of upper and lower cases
Password Age	Reduced password changes from every 90 days to every 270 days.
System usage	Allowed passwords to be used for up to two systems/ applications for some members of the user community
Password History	Reduced password reuse from 2 years to 18 months
Common Usage	Maintained same policy: Passwords cannot be found in either Webster's Dictionary or the King James Bible.
Personal Information	Maintained same policy: Passwords cannot be based on users' or family members' names, birthdays, social security numbers, or other easily obtainable information.

Revised password policy

These simple changes, coupled with a phased rollout to the users (passwords were reset on a group-by-group basis over 30 days) and limited end user security awareness training, resulted in high levels of end user acceptance and an extremely successful implementation.

We also planned for a migration to his stronger password policy over several years. We've found that this phased approach is a more successful mechanism in organizations that have the largest divide between where the organization is and where the organization wants to be.

### Balance is the key

Key to strong security is balance (Yin vs. Yang): asset value vs. acceptable risk, policy vs. usability, and benefit vs. expense. Before presuming that "industry best practice" is the optimal solution for your organization, review the business requirements, consider the gap between your current policy and where you need to be, ensure that the benefit justifies the real costs, and adapt industry best practice to one which is appropriately balanced for *your* organization. Finally, if the gap is

large, take a slower, phased approach.

Remember the Chinese proverb, "Be not afraid of going slowly; be afraid of standing still."