

Case Study: University of California Password Resets

BACKGROUND ON INTERNAL CONTROLS

Internal controls are set up to reduce or prevent fraud, loss and abuse. Because management is faced with limited resources, it is important any new control be evaluated to assure the benefits of the new control exceed resources used. I.e. Management should analyze the costs benefits before changes are made and again analyze the costs and benefits after a period of time to determine the continued cost effectiveness of the control.

Too often there are controls or change to existing controls recommended without consideration of the either the cost or the benefits. Also, often the controls or changes to controls are implemented without a cost benefit analyses. In today's world where threats are increasing it is important the resources are used in the best way possible.

There are several problems in the evaluation and decisions related to controls. There is a challenge in determining the benefits that could be received from controls: there is little research that provides reliable statistics that could be used to show the relative effectiveness of a control; and the nature of managers to be risk when making control related decisions. While there is often little risk to implementing an ineffective control, there are often significant consequences including loss of job on a failure to implement an effective control.

Most controls target loss prevention, therefore to calculate the value of the control, two conditions should be evaluated: the losses (or expected losses) before the control is implemented and the losses expected after the control is implemented.

As an illustration, suppose the manager of a minor league ballpark noted that at every game some teenagers were going through a hole in the fence rather than paying for a ticket. The cost to the ballpark could be calculated by taking the number of people going through the hole and multiplying it by the revenue from a ticket to give a total loss. (This assumes that these teenagers would all buy a ticket). This gives a total loss for the existing state. To add numbers to the illustration, suppose there were 15 teenagers going through the hole bypassing the ticket booth, tickets were \$10 each thus the total loss is \$150.

To find the net benefit for a second state with a new control in place, recalculate the loss with the control in place. In this case, an 8 foot fence would prevent any teenagers from going through the hole, thus the calculation would look like -0- teenagers times \$10 a ticket giving a total loss of -0- dollars. This is a change of \$150 loss difference between the first and second state. However, the second state requires a cost to be incurred. If this 8 foot fence cost \$100, the net benefit would be \$50. (total loss \$150 less the cost of the fence of \$100 giving a net \$50 benefit). Building an 8 foot fence seems like a good decision after evaluating the change in the loss and the cost to implement the control (the 8 foot fence).

Suppose the fence is built, and no teenagers come through the hole thus there are no losses. However, a consultant or auditor recommends that instead of the 8 foot fence a 12 foot fence should be built because it would provide a better control. After all, if an 8 foot fence is good, a 12 foot fence is 50% bigger and thus probably better.

The calculated state with the 8 foot fence has -0- teenagers going through the hole times \$10 a ticket thus a loss of -0-. The expected loss with a 12 foot fence would also be -0- teenagers bypassing the ticket counter times \$10 a ticket, thus a benefit taller fence of -0- (-0- net loss with the 8 foot fence and -0- net loss with the 12 foot fence results in a -0-

benefit for changing to the 12 foot fence.) However, the 12 foot fence comes with an additional cost to change the 8 foot fence to a 12 foot fence of \$80. This cost does not provide any additional benefit, so the result of changing to the 12 foot would be a \$80 cost without any benefit. (The -0- benefit from the change to 12 foot less \$80 additional cost gives a net loss of \$80)

This illustration clearly shows the benefit of the control for an 8 foot fence and the lack of any additional benefit of increasing the fence to 12 feet. This is similar to the recommendation for reducing the time interval that users must change their passwords. While reducing the time between forced password changes seems to be an improvement, it is a change without value.

PASSWORD CONTROL: FORCING USERS TO CHANGE THEIR PASSWORD

Our external auditors recommended at one location to change interval of forced password changed from 90 to 60 days. The same audit firm recommended a second location to change the interval from 60 to 30 days. When asked the basis for the change, they stated "best practice" When challenged for any solid research or evidence for such a change, the audit firm, even after consultation with their internal experts, could offer no additional rational other than everyone thought it was a "best practice".

We felt the "password change interval" control should be evaluated because we have many systems that depend on the integrity of the passwords to prevent fraud, waste and abuse. First we tried to identify research by others regarding the most effective password change practices. While there was guidance on this issue from a variety of sources, none of this guidance appeared supported by any type of empirical research. Without outside research, and because password integrity was an important control, we went forward with our own informal research to try to determine the optimal password change interval. The best model seemed to be a "cost benefit" model

Similar to the illustration of the ball park above, we took the same approach in evaluation the value of changing the frequency of forced password changes. The existing state of our environment included passwords change intervals from 60 days to those that never changed. We then considered the number of incidences that resulted in any type of fraud, waste or abuse that would not have occurred if the password change were more frequent. Lacking a formal recording of such incidences, we relied upon the memory, both ours and other knowledgeable individuals to determine the frequency of such incidences that could fit into this category. These people included the CIO with over 30 years of experience, several security professionals with a combined experience of over 50 years, an IT auditor (me) with over 20 years of experience and various other individuals involved in the security environment. Because this query included a wide variety of systems in a wide variety of environments with a wide range of password intervals we felt this would provide an adequate basis for determining what at what range forced password changes would start to be effective.

This work resulted in zero (-0-) incidences where fraud, waste or abuse could be attributed to the failure to force password changes on a regular interval. The original queries were over three years ago, and I have continued to try to identify even a single case where forcing a password change would have prevented or reduced a loss. I have spoken with many security and audit professionals regarding this matter and have still not been able to find a single case.

The result, if there are zero incidents with the existing state, there is no value to changing the control to be "better" by forcing a more frequent password change interval. (Zero incidents times an unknown cost equals -0- benefit).

We did identify some additional costs that would be incurred if a shorter forced password change interval were implemented. These include cost to change software, additional cost to respond to help desk inquiries and potentially an increased risk with people writing down passwords.

In conclusion, there is no benefit in forcing users to change passwords on a regular basis.

Comment [I1]: Do you force users to change passwords at all? If you do, what is the interval?

Our work did not extend to the relative merits of other password controls; however incidents where sharing passwords allow an individual to bypass application security to enable the person to perpetrate a fraud are not uncommon