Hidden Costs of Passwords

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Many users who focus on their individual experience and needs rather than on corporate security management think that passwords are free. Indeed, password functions come with our operating systems and much of our software; we don’t have to pay anything extra to buy this form of authentication. However, both common sense and research findings support the view that authenticating identity using passwords is a significant expense for organizations.

The major issue is forgotten passwords. Users who lose track of their passwords may have access to an automated password-resetting process, in which case costs may be modest. For example, it is possible to set up a one-way encrypted database of personal information questions and answers and have the user answer a number of these to authenticate to the system. One example is the M-Tech Identity Management Suite™ (<http://psynch.com/features/self-service-password-reset.html>) which provides precisely this functionality (among others) to avoid Help Desk involvement in password resets.

Even this process has a modest cost that depends on the cost per minute of salary and extended costs (relating to costs of facilities, supplies, services and their financing) for the forgetful employee’s time. I’ve always been told to estimate extended costs at around 50%, so someone earning $80,000 a year (for 2,000 hours of work) might be costing the employer around $1/minute. You can do the rest of the math.

The cost grows if the Help Desk gets involved, especially if there’s a lag in responding to the emergency call. In addition to the cost of the Help Desk personnel’s time (which one can either include or discount as being paid anyway, depending on the point of view), the big cost begins to be the ticking clock as the locked-out user waits for a reply. For the $1/minute employee mentioned above, a five-minute wait twiddling her fingers amounts to $5 of wasted costs – but a half-hour delay is $30. Do you ever have to wait half an hour for a callback from the Help Desk?

Multiply the lost passwords by the number of employees and the average number of times people forget their passwords and you can see that the costs begin to rise significantly. At some point, tokens and biometrics begin to seem less expensive, comparatively, than they seemed at first glance. In a 2005 article, Lisa Phifer writes, “According to Burton Group and Gartner studies, password resets represent 30 percent of all help desk calls. The META Group estimates that each help desk call costs $25.” (<http://www.isp-planet.com/technology/2005/beyond_passwords_1a.html>) In a white paper by RSA (makers of cryptographic tokens, remember), the authors claim that for a 1,000-user organization, the total cost of ownership over the first three years is around $673,000 or $673 per user. About 98% of that depressing expense is due to management costs.

Similar calculations are shown in a Cost of Ownership (ROI) document from RoboForm. (<http://www.roboform.com/enterprise/solutions/costofownership.html>) The makers of this single-signon solution estimate cost savings of about $417 per user in the first three years for a 1,000-user organization through reduction of lost-password calls.
Avatier, makers of the Avatier Password Station, have placed an ROI Calculator for their product on the Web. [http://www.avatier.com/products/PasswordStation/ps_cost_analysis.html] It allows you to enter the number of employees, the number of Help Desk calls per user per month, the duration of Help Desk calls, the hourly costs of both Help Desk staff and callers, the percentage of Help Desk calls relating to password reset (30% on average according to Gartner Group) and the percentage of users who will use their product. The calculator shows the ROI in months, total cost savings in year one and total cost savings by the end of the third year.

I suggest that you take the time to examine the resources above and others you can find online. And the next time some innocent challenges you about how “free” passwords are, you can discuss the issue with a more realistic perspective than they bring to the table.

[MANDATORY DISCLAIMER: I have no financial relationships whatever with any of the companies mentioned in this article.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance [http://www.graduate.norwich.edu/infoassurance/] and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.