



## 24 Real Costs Resulting From Password Issues

PistolStar, Inc.  
PO Box 1226  
Amherst, NH 03031  
USA

Phone: 603.546.2300  
Fax: 603.546.2309  
E-mail: [salesteam@pistolstar.com](mailto:salesteam@pistolstar.com)  
Website: [www.pistolstar.com](http://www.pistolstar.com)

## 24 Real Costs Resulting From Password Issues

1. End-users experience confusion and frustration dealing with different password complexity rating scales and need to be educated on the complexity ratings — a tremendous time sink.
2. Lacking secure and controlled end-user access and possessing weak password policies can affect an organization's compliance with governmental regulations.
3. Experiencing repeated logins every time they launch applications reduces end-users' efficiency as it complicates the login process and increases overall login time.
4. Having multiple passwords and usernames to commit to memory increases the likelihood end-users will jot them down on notes, exposing them to internal hackers.
5. With so many passwords being used that correspond to various systems, password policies — specifically, password quality and password expiration settings — tend to differ, which can complicate password synchronization.
6. When password synchronization is interrupted, the authentication process becomes slow or does not even occur, preventing the end-user from gaining access to their applications and forcing administrators to spend time resolving the resulting chaos.
7. The security of critical corporate files and data is compromised when network intruders or hackers can gain access by guessing passwords. (Guessed passwords are among the most common threats to corporate security, accounting for nearly a quarter of all network attacks.)
8. Administrators' passwords can be weak and thus easily seized by potential intruders or hackers to gain access to systems.
9. Both end-users and administrators sometimes share their passwords with co-workers and friends, which compromises security because those passwords can ultimately end up in the hands of an unauthorized person.
10. End-users typically choose passwords that are easy to remember, but these passwords are also easy to guess and therefore not secure.
11. End-users can resort to employing commonly used passwords such as "abc123," "123456," "letmein" and "password1," making it easy for others, specifically intruders and hackers, to figure out their password.
12. Self-service password resets often necessitate using a different machine to access a portal, requiring the end-user to login using a guest account and a publicly known password. In addition to being a security concern, this creates an inconvenience that interrupts two end-users' workflow and lessens productivity.
13. The configuration of separate password policies for Windows, HTTP and Lotus Notes ID passwords requires administrators go to multiple locations to set password expiration and complexity, adding more tasks to an already heavy workload.
14. Because of the plethora of software tools and applications for which end-users have passwords, repeated calls to the Help Desk to reset forgotten passwords strains IT resources.
15. As a consequence of requiring administrators to perform password resets, organizations can have one or more individuals who possess knowledge of all the end-users' passwords.

16. In addition to passwords, end-users possess several different usernames, which can also be forgotten or confused with passwords, generating even more calls to the Help Desk.
17. The task of remembering multiple passwords and usernames is an inconvenience for end-users that consumes their time and energy and decreases their productivity.
18. The complicated and time-consuming steps for recovering the Lotus Notes ID password create excess work for IT administrators and a drain on IT resources, as well as a large amount of downtime for the end-user.
19. The responsibility of addressing password issues and ensuring passwords are secure is a time-intensive endeavor for administrators that diminishes their productivity.
20. Performing password resets on a regular basis robs IT administrators of time and resources that could be spent on more important IT or security matters.
21. End-users experience a sizable loss in their productivity as a result of downtime waiting for administrators to reset or recover forgotten or lost passwords.
22. The dramatic reduction in both administrator and end-user productivity increases IT and staffing expenses, ultimately impacting the bottom line.
23. Downtime experienced by the end-users and administrators because of password issues means lost time for the organization.
24. When passwords can be lost or stolen easily, they not only become less secure, they pose a risk to the organization.

### **PistolStar Password Power 8 Plug-In Market**

Web Set Password was among the first products developed by PistolStar in 2001 and is one of the company's Password Power Plug-Ins. Developed to respond to the tremendous need to secure IBM Lotus technology while simplifying the logon process, PistolStar's Password Plug-Ins have become leading solutions in the IBM Lotus Market. Since 2001, PistolStar has sold its password authentication and management products to hundreds of enterprise-level companies with an average of 7,000 users, demonstrating that a need exists for these types of security solutions in corporations worldwide.

While PistolStar continues to expand its presence in the enterprise market, it is also focused on meeting the needs of the small-to-medium business (SMB) market. PistolStar serves an international customer base across a range of vertical markets, including automotive, chemicals, consumer products, finance/banking, government, healthcare, manufacturing, advertising and media, communications, pharmaceuticals and retail. Overall, about 75% of PistolStar's customers are U.S.-based organizations and 25% are international.

PistolStar offers true value to customers by responding to their needs and feedback with customized solutions and the product capabilities that will provide the most benefit. PistolStar is focused on delivering refined, yet complete, feature sets that yield precise results.

For more information, contact PistolStar at 603-546-2300, or visit the PistolStar Website at [www.pistolstar.com](http://www.pistolstar.com).

###