



Data Security for Executive Directors and “Dummies”

An Overview: Securing Financial Information

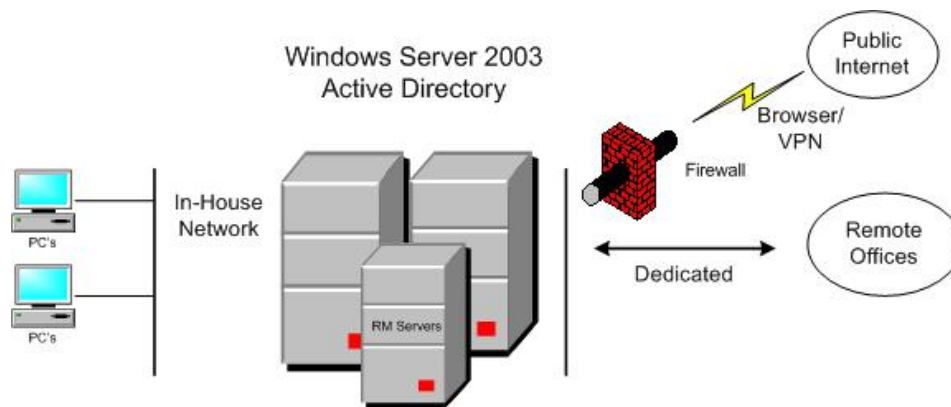
By, Jim Hammond, President, RainMaker Software, Inc.

www.rainmakerlegal.com

Firm administrators need to understand the basic concepts of securing financial data, along with the practical considerations of making it readily available to end users while keeping IT costs under control.

Start With Active Directory

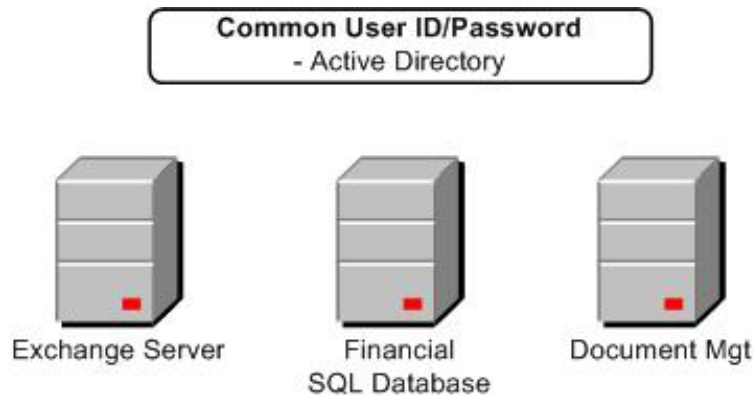
Let's examine data security from the very top. Microsoft® Active Directory (AD) provides for a full suite of administrative capabilities including the common sharing of all user login names and passwords. This allows the firm to have mobile workers who can access system wide resources assigned to them whether they are working from their personal desktop PC, a remote office PC or connecting from home via VPN. AD also allows a firm's network administrator to set network policies, control and automate local PC Windows updates and perform remote diagnostics throughout the entire firm and remote network locations.



Add “Windows Authentication”

Now that the overall network is secured it's time to examine specific software applications. The legal industry standard for storing financial information (at least in mid-to-large sized law firms) is by incorporating a Microsoft® SQL Server database(s). Many vendors utilize the standard built-in security called Microsoft® SQL Server Authentication that prompts users to login and provide a password. Microsoft® SQL Server Authentication relies on the internal user list maintained by the Microsoft® SQL Server computer. Unfortunately, this list does not include Microsoft® Windows network users, and is specific to the Microsoft® SQL Server computer. Therefore totally separate lists must be maintained and updated by the IT staff. Furthermore, if your vendor provides multiple points of application access, like web based products accessing separate Microsoft® SQL databases such as a data warehouse, users must potentially login multiple times.

Software vendors can provide a much more integrated security solution by adding a "Windows Authentication" (Active Directory). Microsoft® SQL Server has the ability to recognize Windows Authentication and pass-through common user logins and passwords. The bottom line is Microsoft® Windows Authentication allows the firm to manage one level of common user logins and passwords, and yet provide highly-secured access to Microsoft® SQL based information. Vendors adopting advanced technology can design their systems to allow a user to login to any single application first and then access the second application, web based inquiry for example to identify the users security credentials automatically and bypass the second login screen.

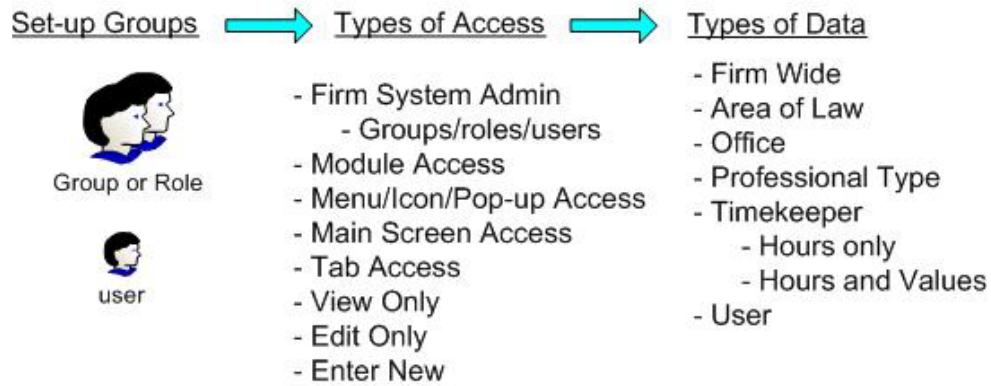


Application Level Security

At this point, we have secured access to our specific application such as our Time and Billing system. Well-designed software will allow for the setting of layered security.

1. Group or role-based security allows the firm to define the roles people play in their daily functions, such as an accounts payable person, a billing person, an attorney, etc. Some groups will have very wide access or system administrative rights to all or most of the system. Once groups are established, individual users can then be assigned to each group. Custom settings allow individual users to be in a group all by themselves. Most systems allow copying settings from one group or user to another to facilitate the set-up process.
2. The security model will now allow the firm to decide what module, menus and beyond access each group will have. This can carry all the way down to view vs. edit/add new data access on each tab or menu within a specific application screen. For example, attorneys can view collections activity for their clients but secretaries cannot.
3. The level of financial roll-up is the final level of security for a user in financial inquiry type modules. For example, in a web browser inquiry:
 - a. Can an associate see a partner's billable hours and value?
 - b. Can an attorney view his own information as a billing, originating or other attorney type?
 - c. Can a partner see some office or area of law roll-ups on a selective basis?
 - d. Should some partners access firm-wide information?

Application Level Security



Summary

The right combination of network design and vendor software will provide your firm with a high degree of security, lower IT costs and control access to information by the end users.

About the Author

Jim Hammond, President, RainMaker Software Inc., has more than 25 years of law firm software experience. RainMaker provides mid-to-large sized law firms with proven, practical and progressive Financial Management, Practice Management, Business Intelligence and Case/Matter Management software. He can be reached at jhammond@rainmakerlegal.com.