BoardBook Security Questions:

How is BoardBook's Web infrastructure physically secured?

The BoardBook servers are housed in a primary server room, which is located on an upper floor in an inner core isolated area with no external access. This room is structurally self-contained and secured by metal doors with centrally controlled electronic locks. It is protected by dual independent sensor alarm systems for fire, smoke, water, and noise that control a system to provide full room fire suppression.

Electrical power for the servers is conditioned and provided by a two-level Uninterruptible Power Supply (UPS) architecture that allows a run time of approximately 90 minutes followed by an orderly shutdown.

The BoardBook servers are rack mounted server class machines with redundant UPS/power supplies and hot-swap raid protected disk drives. The environment is monitored 24 hours a day and is supported by certified hardware and software engineers.

Data backups are performed nightly as part of a three-tier backup system with media rotated among a secured separate storage room in the same building, an inner core secured room in a separate building, and a remote secured storage facility.

Applications and facilities required by BoardBook are part of a formal Business Continuity Plan that is reviewed and tested on a regular basis.

How is BoardBook data secured?

The overall Internet network environment is protected by a configured restricted router and proprietary software firewall, which is tested several times a year by third party “white-hat hacker” consultants. Access to BoardBook data and applications is controlled by an application level proprietary control system based on unique user ID/password.

Data transmitted over the Internet is encrypted via SSL, and BoardBook databases are restricted at a file level on secure servers.

Virus protection is provided by a three-tier multivendor architecture using a proprietary entry point virus appliance, server disk scans, and local desktop scans.