Security of the NSSE Computing Environment

NSSE is administered by the Indiana University Center for Survey Research.

The computing environment at the Center for Survey Research (CSR) requires a high level of computer and data security. The University Information Technology Services of Indiana University provides an initial level of security including protocols to prevent unauthorized access to Indiana University computers. The CSR computing staff uses industry standard best practices as our security procedures. Each CSR workstation is updated daily with virus protection software. The CSR network is scanned daily for needed security packs and patches. The security server deploys all needed Microsoft security patches each night. Once each week, all workstations receive a complete scan for possible security problems. We have experienced minimal disruption due to viruses or worms.

The computing staff has designed a number of processes for preventing intrusions or data loss on the CSR's servers. Access to the servers is tightly controlled by user IDs and passwords. Access to directories on the file servers is restricted to only those employees who need to use them. Security processes similar to those run on the workstations are used to prevent, detect, and repair security problems on the servers. Firewalls are used to detect and prevent unauthorized intrusions. Indiana University provides scanning of our servers to look for possible problems and the computing staff carefully monitors server event logs for possible attempts at intrusions.

The files on the servers are backed up each night, and complete system backups are done weekly. The file and Web servers use RAID 5 technology to insure that a disk failure will not cause any loss of data. The servers have uninterruptible power supplies. The server room is on a separate lock from other doors in the building, and there is a motion alarm in the room.

The CSR uses 128-bit public key encryption and digital certificates to ensure the security of survey and other sensitive data that are transmitted across the Internet. The digital certificates were issued by VeriSign and Thwate and are used by the survey respondent's browser to authenticate the CSR's website before transmitting data. The data are encrypted using public key encryption before they are sent over the Internet. Through the use of these protocols, the data are transmitted using the SSL. The security procedures used by the CSR are equal to or surpass the requirements for transmitting confidential information.