Computer Security

The survey facility is located in a secured building in downtown Gainesville, Florida. The CATI software used to conduct phone surveys and enter mail responses, using Wincati sample management and Ci3 questionnaire authoring, runs on a file server that is dedicated to this purpose in a virtual machine environment. No other IT services are run from this server. Backups are performed nightly and maintained offsite in a secured room with a redundant power supply.

The state-of-the-art voice-over-Internet protocol (VOIP) telephone system uses Asterisk open source technology. This allows us to record 100% of the phone calls for quality control purposes. Our system also facilitates live monitoring during shifts and allows clients to conduct real-time monitoring remotely.

The survey lab includes 93 telephone interviewing stations separated by sound-absorbing carrels. All interviewing stations are networked to a Windows 2008 R2 file server, with 350 gigabytes of disk space, using two voice T1 lines, plus one data T1 line directly connected to the Northeast Regional Data Center with an Internet connection. The network switches we use are CISCO fault tolerant. Each of our stations has an Intel CPU running with Windows 7, and is configured with soft-phones and headsets.

We have an onsite IT staff plus five BEBR staff members who are able to help with any issue that may arise. As part of the College of Liberal Arts and Sciences and the University of Florida as a whole, the UFSRC can call upon the services of additional technical support personnel including, but not limited to, computer support and data processing. Having purchased our network switches through UF, we also use their staff as technical support for network problems.

The security of data collected is a priority for the UFSRC. The servers are kept in racks, behind three sets of locked doors with keys which are controlled. All staff is trained to question anyone who requests access to the server room and to inform the IT staff.

Our survey research databases are maintained on a Microsoft Windows 2012 server. A router is configured with narrow access control lists that are set to block all traffic from the campus network except from specific ports to specific servers. The survey research databases cannot be directly accessed from computers outside our local area network.

The Systems Administrator restricts access to the UFSRC computer system through a user list maintained in Active Directory. All client computers are connected to managed switches that are monitored for event logs for multiple failed log-in attempts to detect unauthorized access 24 hours a day, seven days a week, by the BEBR IT department.

Interviewer workstations are locked down and the firewall blocks anyone logging in as an interviewer from accessing the Internet. Interviewers can only run approved programs that are relevant to the data collection job. Interviewers must log off when leaving the area, and workstations automatically lock after three minutes of inactivity. We have off-site back up as well as fault-tolerant disk arrays in secured room. A firewall and access control lists separate the file server from the Internet, allowing System Administrators a set of tools for limiting access and preventing unauthorized break-ins.

Password requirements:

1. Password must have a minimum length of 8 characters.
2. Passwords can have a maximum age of 365 days.
3. Password minimum age for reset: 1 day.
4. Password uniqueness/history: 200 days.
5. Failed attempts before lockout: 10.
6. Lockout duration: 30 minutes.
7. Password composition rules require the inclusion of 3 of the 4 following character sets: lowercase letters, uppercase letters, numerals, and special characters. Allowable special characters are ~ ! @ # $ % ^ & * ( ) _ + | – = \ { } [ ] : ” ; ‘ < > ? , . / and the space character. Passwords may not include words of more than 4 characters, as tested against a dictionary of at least 50,000 words.
8. The selection of a pass-phrase of at least 18 characters eliminates the password composition rules and dictionary check. Pass-phrases are subject to minimal tests to prevent use of common or trivial phrases.

All computers and servers are scanned regularly for security patches and breaches. Patching is carried out by automated services complete with reporting of failure and successful patching. Any failures are corrected or taken offline until corrected. Any compromised computer is taken offline for forensics and will be completely reimaged before being used again.

We use a fiber connection to link back to the campus network. The speed is 1 GB/s for incoming and outgoing traffic. The file servers and network switches are all connected to battery backup systems.