TOSHIBA

STRATA® DK
SALES BULLETIN

SBDK-0001
September 26, 1994

FRAUD PROTECTION WITH BUILT-IN AUTOMATED ATTENDANT

Telephone fraud prevention is a concern to everyone. Every telephone system is potentially susceptible to unauthorized outside entry by telephone use thieves or “hackers.” Outside entry through Voice Mail, built-in Automated Attendant, DISA, and Remote Maintenance must be closely controlled. Proper management of passwords and security access codes is the main factor in minimizing the risk of telephone fraud.

To assist this process, Toshiba published a Technical Bulletin in June 8, 1992 (TB96-0001, Item #4031004). It described various procedures and recommendations to assist in the prevention of telephone fraud. The purpose of this new bulletin is to further supplement this information.

DISA ACCESS VIA BUILT-IN AUTO ATTENDANT

When a call is answered by the Strata DK built-in Auto Attendant, the caller can press the “*” button, and get “DISA dial tone.” At this point, they can access all facilities available to DISA users. It is important to note that this is possible even if individual DISA lines are not programmed for use within the system. This means if no DISA security code is defined in the system, the caller does not have to enter a security access code, and will be able to make unrestricted outgoing calls, assuming they know feature and/or CO line access codes and dialing procedures.

> ***If outside lines are designated as DISA lines, a DISA security code of at least 6 digits (1-15 digits available) should be assigned. For the same reasons, a DISA security code should be implemented whenever the built-in Auto Attendant is used with Strata DK systems. This is necessary whether or not the DISA feature is actually being used, and even if CO lines have not been programmed for DISA. Otherwise, outside callers can potentially gain unauthorized access through the Auto Attendant.***

RECOMMENDED ACTION

For all Strata DK systems using the built-in Auto Attendant, a DISA security code should be defined and properly managed, regardless of whether the DISA feature is used. For all Strata DK systems, the user can freely change the security code at designated stations. It is also recommended the customer change security codes on a regular basis. Full details are contained in the System Administrator’s Guide. Therefore, no service call or site visit is required.

SUMMARY

Strata systems provide various security levels to help control access within the customer’s environment and minimize the risk of unauthorized outside access. Selling these security features can help you create differentiation from your competitors, and make your customers feel more confident that the potential for abuse of their Strata telephone system can be minimized.

Of course, there are no guarantees against telephone hackers and telephone fraud. There are only reasonable measures that help customers minimize their risk. These security features must be implemented during installation and are only as good as the procedures that control them on an ongoing basis. Judicious use and periodic changing of various types of security codes is very important. The better job the user does of administering these security features, the more secure their system will be from unauthorized access and abuse.

Be sure your existing Strata DK systems have a DISA security code. Contact your customers today . . . they’ll thank you tomorrow!