



Subject Line: Info Security - Commit and Manage

June 29, 2006

Dear Real Estate Executive

Laying the foundation for effective information security management is the most important factor in protecting information assets. **You must make a conscious decision to make information security a priority in your business.** Then you have to sustain that commitment with continued executive sponsorship, policies and procedures, and ongoing resource allocation.

The business of real estate today is dramatically different from even five years. Information security is now an important and required management issue.

Security failures can be costly to any real estate organization. Losses may be suffered because of the failure itself, when recovering from the incident, or by the costs to secure systems and prevent further failure. For information security to be successful, information security management should be established and communicated clearly to all parties. Key elements include:

**Senior Management Commitment and Support**—Executives must deliver a consistent message on the priority placed on protecting information and assets. Your intent must be clear and your goals for information security explicitly stated. Senior leadership must “walk the talk.” This includes funding and resources necessary to meet those priorities and goals.

**Policies and procedures**—Policies and procedures start with a general organization policy providing concise top management declaration of direction. Your policy must reflect the importance or value you place on your information, how you define sensitive or critical data and assets, and how you protect the confidentiality, integrity and availability of that data and assets.. Once a policy has been approved and roles and responsibilities assigned, it is necessary to develop information security management procedures and use standards that can govern development of minimum-security baselines.

**Organization**—Finally, you have to identify who is going to be responsible for information security. Responsibilities for the protection of data and other

information assets and for carrying out specific security processes (e.g. system back ups, surveillance camera maintenance, hardware inventory) should be defined clearly. This should be supplemented, where necessary, with more detailed guidance for specific sites or services depending on the size and complexity of your organization. Finally, employees should know who the “information security team” is and what they do.

Information security is a business imperative that cannot be addressed by simply hiring information security professionals or applying technology. The ability to properly identify risks to information and assets requires collaboration from agents and executives alike.

Most important, is the need for executives to support the tough decisions with regard to protecting information and assets.

Mark Lesswing  
Vice President  
Center for REALTOR® Technology  
[mlesswing@crt.realtors.org](mailto:mlesswing@crt.realtors.org)

REALTOR® Secure program resources  
<http://www.realtor.org/crtsecure.nsf/pages/resources?OpenDocument>

Information Security Management Handbook  
<http://www.ccert.edu.cn/education/cissp/hism/ewtoc.html>

Information Security Management Challenges  
<http://www.cert.org/archive/pdf/ESMchallenges.pdf>

Security plan enforcement  
<http://www.computerweekly.com/Articles/2006/06/08/216326/Enforce+your+security+plan.htm>