

Secure Content Group



Perspective...

Vol. 1

The Changing Risk Equation

All real estate organizations are in the risk management business. The risks associated with managing the confidential information of consumers and trading partners cannot be taken lightly. Recent events and media coverage indicate a sea change in consumer expectations and a growing list of e-commerce liabilities. The simple equation below is an effective method to quantify risk:

$$\text{Risk} = \text{Threats} * \text{Vulnerabilities} * \text{Asset Value}$$

New threats and ever changing vulnerabilities combined with an acknowledged increase in the value of digital assets have changed the risk equation for all industries. As a result, information security has been among the fastest growing of all IT expenditures. In the pre-Internet era the risks for real estate organizations were easily contained making significant investments in policies, practices or technology difficult to justify. The potential to irreparably harm the business operations of companies, business partners and consumers has opened the doors to **new risks** for every real estate broker doing business on the Internet.

Real estate organizations are facing several **new threats** to their market position resulting from their inability to control their information, including:

- Third Parties who obtain real estate content for referrals and other purposes.
- Practitioners and contractors who disclose or misuse real estate content
- Attackers who pirate all forms of information that are poorly protected
- Data Resellers who blend real estate with other forms of consumer information
- Lenders who are positioned to integrate and extend the value chain
- Government that is actively considering security and privacy regulation
- Service Providers with the capability to manage transactions on behalf of consumers

The vulnerabilities in the security architecture of real estate are growing. What is also clear is that the value of real estate content, such as listings and consumer profiles, continues to escalate along with the

cost of new systems and software to manage it. Together these factors have **altered the balance**, leaving brokers substantially disadvantaged against the known threats.

Contractual and regulatory liability, disruption of business operations, loss of public confidence, reduced commission rates, losses from theft and fraud are a few examples of risks that can be quantified.

Transaction management will introduce new risks and expose many of the open windows in the industry's security architecture. Policies are needed to assure identity, protect the integrity and confidentiality of information, and specify liabilities between trading partners when incidents occur.

Approaches to help contain the risks of brokers within a market area will vary, but there are certain fundamentals that must be adhered to. Comprehensive security policies must be enforced with contractual protections, and supported with education, training and technology. Brokers must evolve toward a new **risk management framework** that begins to approach how financial services firms deal with sensitive information.

Additional investment will be required but a sensible, balanced information security program can yield a dramatic return on investment. Brokers are faced with the opportunities to enable paperless transactions, create new marketing models, reduce operating costs and increase market share. Each of these business drivers requires the **inherent capability** to create, manage and exchange information...in a secure manner.

Term	Definition
Risk	The probability that a particular threat will exploit a particular vulnerability of the system
Threats	Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service
Vulnerabilities	Hardware, firmware, or software flaw that leaves an AIS open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing
Assets	Information or resources to be protected by the countermeasures of a system

Secure Content Group serves associations, government, financial services, pharmaceuticals and real estate. Read more about Secure Content Group's unique perspective on digital governance in real estate.

Jack Horton Managing Partner 703.909.2427

J.T. Hardy Partner 240.351.6955

Contact info@securecontentgroup.com

visit our site: www.securecontentgroup.com

