

## **“Open Window” A Cautionary Tale**

It was like any other day until the broker's assistant said an **FBI agent** wanted to see him. The conversation was brief. What did the broker know about John Doe, an employee of the contractor who was running his IT system? Apparently Mr. Doe had disappeared, leaving evidence that he was part of a potentially dangerous identity theft ring. The FBI asked if the broker would cooperate in the investigation, or would they need a court order to look at his security policies, practices, contracts, system logs, audit results and company records.

He called his lawyer who couldn't imagine how a real estate broker could be “of interest” in a large scale identity theft investigation. Within two hours a forensic team finds traces of a new virus that had been embedded across the broker's business applications. A file of new listings had been uploaded to the MLS and a communications port opened, **exporting** all of the broker's customer, financial and employee information to an offshore web address.

The MLS had broadcasted the infected file everywhere and there are indications that other brokers are similarly affected. Agent websites are being spoofed, asking consumers for credit cards before displaying listings. The virus has been tracked all the way to Realtor.com, regional MLSs, banks, title companies, major newspapers and advertising sites like AOL and MSN. The FBI and Secret Service are astonished by the reach of real estate information. They have seen many industries that are as **interconnected**, but none as vulnerable.

Coverage of the widening event leads the local 11 o'clock news, and worried buyers and sellers begin calling their agents. By comparing customer files with credit bureau records, investigators are able to determine that a **harvesting operation** has been churning for some time; changing addresses, ordering credit cards, buying merchandise, applying for driver's licenses and obtaining new social security cards. The breach is estimated to already involve over 200K Americans. The broker's small business is unwittingly the index patient of a growing epidemic.

The next day the broker's franchise company finds gaps in their financial records, it's almost as if something is eating through them. At MLSs, the same thing is happening to listings and transaction records. Phone calls from hysterical brokers around the country indicate that the entire **info-grid** of the industry has been contaminated. Later that next day a malicious payload detonates, the information assets of brokers and MLS that were not backed up...vanish.

The outcry is a public relations and stock market disaster. Brokers are stunned by the impact of an event that is typically associated with major portals, commercial information companies and banks. They realize that their **open windows** made them an inviting target. A class action law suit is initiated. News reports describes all the proven methods that could have deflected or contained what is becoming the first industry meltdown. Many MLSs were unsuspecting threat multipliers, unaware of security policies, practices and technologies widely employed by other industries. Firewalls and penetration testing did nothing to prevent an internal attack.

Legislation passes quickly to make brokers subject to the security regulations of financial services firms. The brands of the best known brokers are punch lines for late night comedians, and several prepare to face Sarbanes Oxley 404 prosecution. Only a few MLSs remain in operation. Consumers begin to migrate to FSBO sites that secure their information and are certified by trusted third parties. Membership in real estate associations plummets, leading to

consolidation and a new appreciation of our national dependence on the **safe exchange** of information.