Cyber and Data Security Risks

and the Real Estate Industry

by:

Joe Fobert
Real Estate and Retail Industry Practice Leader
Real Estate Practice Group, AIG Property Casualty

M. Leeann Irvin
Director
Issue Management, AIG Property Casualty

Chris Andrews
Assistant Vice President
Financial Lines, Lexington Insurance

Steve Kammann
Financial Institutional Division
Financial Lines, AIG Property Casualty

Cyber and Data Security Risks and the Real Estate Industry

The risks associated with data security and cyber breaches continue to grow, impacting a variety of industries worldwide. Cyber criminals have become more creative and their attacks increasingly destructive, targeting organizations of all sizes. These attacks can lead to costly lawsuits as well as first party losses and expenses. Acts of employees, whether malicious or unintentional, are also on the rise. These risks present significant financial and legal exposure to unsuspecting, often ill-prepared businesses. The Real Estate Industry historically has not been targeted as aggressively as other industries, such as retail, financial services and healthcare; however, increasing reliance upon technology within the real estate sector and the fact that real estate firms are creating, using, storing and sharing more information than ever should compel real estate professionals to take a serious look at these exposures and how they are managed.

Data Breaches

Data Breaches are Becoming Commonplace

Data breaches are becoming commonplace. Since 2005, 3,241 separate data breach incidents have compromised a total of 562,943,732 records containing sensitive personal information. According to the Identity Theft Resource Center (ITRC), 419 data breaches were documented in 2011. In 2012, 447 incidents were confirmed. As of March 2013, the ITRC has already reported 109 breaches and anticipates that through 2016, the financial impact of cyber crime will grow 10 percent per year.[1]

In 2012, the Ponemon Institute launched a real time study of cyber crime in the U.S.[2] The 56 participating companies experienced 102 discernible, successful cyber attacks, averaging 1.8 attacks each per week. These invasions included reported instances of viruses, worms or trojans infiltrating the company's computer system; malware, web-based attacks, stolen or lost devices, employee error (negligent or intentional), phishing and social engineering. With criminals stealing everything from customers' personal identity information to bank account details, social security numbers and personal health records, public anxiety is growing almost as quickly as criminals and hackers are devising new methods to infiltrate so-called secure systems.[3]

Real estate firms are affected by this trend. Property managers, brokers/agents, title agents, developers, appraisers, multi-service real estate firms and others may have significant amounts of confidential third-party information, either in the form of personally identifiable information (PII) or confidential corporate information.

Many businesses generally do not recognize the risk of targeting by cyber criminals

"According to a survey conducted by Visa and the National Cyber Security Alliance, more than 85 percent of small business owners believe their companies are less of a target for cyber crime than large companies".[4]

For example, rental applications, credit reports, leases and rental agreements contain personal information of applicants and tenants — precisely the type of information targeted by cyber criminals. It is vital that firms secure these documents against possible identity theft. In fact, the "disposal rule" of the Fair and Accurate Credit Transactions Act (FACTA), federal law enacted in 2003, states that disposal of these records must be through incineration or shredding. Even small landlords are obligated to comply with this requirement and would benefit from a system in place for maintenance and destruction of private data-containing records. In addition to compliance with destruction of paper files, information stored on computers or handheld personal data systems must similarly be preserved and/or disposed of. This can be accomplished through software that automatically wipes information off the hard drive and prevents restoration of material that has been deleted.[5]

Real Estate Investment Trusts (REITs), a multi-trillion dollar industry, own, and in most cases, operate income-producing real estate. Some REITs also engage in financing real estate. Depending on the REIT structure (public versus private) and type of investor (individual, corporation, etc.) information is held electronically or in hard copy by these trusts and can include tax records, federal identification numbers, social security numbers and other confidential information.

Data Loss

In Addition to Cyber Crime, Data Loss Poses Substantial Risk and Exposure for Real Estate Firms, Both Large and Small

For some firms, use of the internet is secondary to their businesses, and many are unprepared to deal with data loss. In a November 2012 report, Symantec found that 80 percent of the data breaches reported in 2012 happened to organizations that did not rely on the internet as a core piece of their business.[6]

These losses result from lost or stolen equipment — even a lost laptop containing personal data. Misappropriated customer or tenant information can result in significant liability for an owner and/or landlord. A 2010 study found 46 percent of the lost laptops contained confidential data, only 30 percent of those systems were encrypted, and only 10 percent had other anti-theft technologies.[7]

In December 2012, a local news station in Fort Myers, Florida ran a story about uncovered boxes filled with private, personal information (including credit card, social security and drivers' license numbers) that were thrown into a dumpster. The files were found by a passerby who was searching the dumpster for moving boxes and reported it to the local news and authorities.

Moreover, storage of information is increasingly being outsourced by real estate firms. In 63 percent of incident response investigations, a major component of IT support was outsourced to a third party.[8] While outsourcing can help real estate firms gain effective, cost-friendly IT services, these firms also need to understand and proactively seek to reduce the risk their vendors may introduce. According to the 2013 Trustwave Global Security Report, of 450 global data breach investigations, 63 percent were linked to third-party IT system administration, support, development and maintenance that had security deficiencies easily exploited by hackers.[9]

The Costs

New Modes of Cyber Attack Suggest the Financial Impact of Cyber Crime Will Grow 10 Percent Per Year Through 2016[10]

While awareness of cyber crime may be increasing, an appreciation of the cost associated with remediating these attacks has been slow in developing. According to the Ponemon Institute, the most expensive cyber attack experienced in their study incurred over $51 million in damages and remediation costs; the *smallest* was still over $1 million. The average expenditure to remediate these attacks was $8.3 million.[11]

In 2011, data breaches cost U.S. businesses $194 per compromised record. Unsurprisingly, costs increase if the attack is not resolved quickly. The average time to resolve a cyber attack is 24 days. The average value of a lost laptop is $49,246 after a data breach, 80 percent of which is for lost data compared to two percent for the cost of replacing the computer.[12]

Further, to investigate and remediate a breach, forensic companies are often hired to identify its source. The cost of these investigations can be in the hundreds of thousands of dollars. Expenses associated with notifying those whose confidential information may have been compromised can also be significant. Responding to breaches may also negatively impact productivity, drawing on crucial company resources in an attempt to respond quickly and effectively. Finally, network interruption could lead to loss of income and generate unnecessary additional expenses for real estate firms who rely on their network to conduct business. Combined, these can amounts reach hundreds of thousands or even millions of dollars, damaging the balance sheets of larger real estate firms and potentially crippling smaller real estate businesses.

Regulatory Issues

Even When a Business is Aware of the Cost of Cyber Crime and/or Data Loss, Most Are Less Aware of the Impact the Ever-Changing Regulatory Environment May Have on Their Bottom Line

Many states are adopting statutory requirements for remediation and imposing fines on companies if data protection is deemed inadequate. Unfortunately, jurisdictional requirements vary, specifying different notifications and measures. Given the growing reach of multi-state and multi-national businesses, rules of multiple jurisdictions are likely to be involved in any one cyber crime or data breach. Even the federal government is getting involved, pursuing civil rights violations and assessing multi-million dollar fines resulting from data breaches against companies, some of which were unaware the data was lost.

Laws governing data breaches are increasingly favoring victims, and judges are recognizing that information has intrinsic, compensable value. As a result, plaintiff attorneys are taking cases with smaller exposures, meaning even smaller real estate firms may not be able to fly under the radar.

Real Estate Examples

Because Real Estate Firms Use an Abundance of the Same Data Criminals Seek, Increasingly They Are Being Targeted

Examples include:

- In March 2012, the Massachusetts Attorney General fined a property management firm $15,000 after a company laptop containing unencrypted personal information was stolen. In addition to civil penalties the company was required to ensure that use of portable devices was limited, information stored on them was encrypted and they were stored in a secure location. The company was also required to train employees on the policies and procedures for securing and maintaining the security of personal information.
- Another real estate specific scam involved rental properties posted online. Cyber criminals copied the digital information from online listings to create their own listing to collect the initial deposit and rent for property they did not own.
- "We will keep your information secure." That was the mantra on which Shawn Poole, the CEO of Employ Bridge, based his company's reputation. But in March 2012, Employ Bridge faced liability after thousands of documents containing personal information were found in a recycling dumpster. The ensuing investigation revealed the documents were taken from the company's office without its knowledge or permission after the landlord believed the lease had ended and had sent a cleaning crew to clean out the offices.
- In December 2012, two people were imprisoned for running a massive identity theft ring in San Diego, California. Much of the personal information is believed to have come from stolen real estate files.

Insurance

The Increase in Data Breaches is Creating a Demand for Insurance Products Covering Such Exposures

AIG has responded to this demand by creating CyberEdge®, a comprehensive risk management solution for cyber insurance offered through various of its subsidiary insurance companies. CyberEdge provides innovative protection to help businesses safeguard against sensitive data breaches, computer hacking, dumpster diving, computer viruses, employee sabotage or error, pilferage of information and identity theft*, specifically providing:

> "Buying some level of cyber liability insurance makes sense, regardless of the size of a company… Every company has some level of private information that can expose them to legal claims."[13]

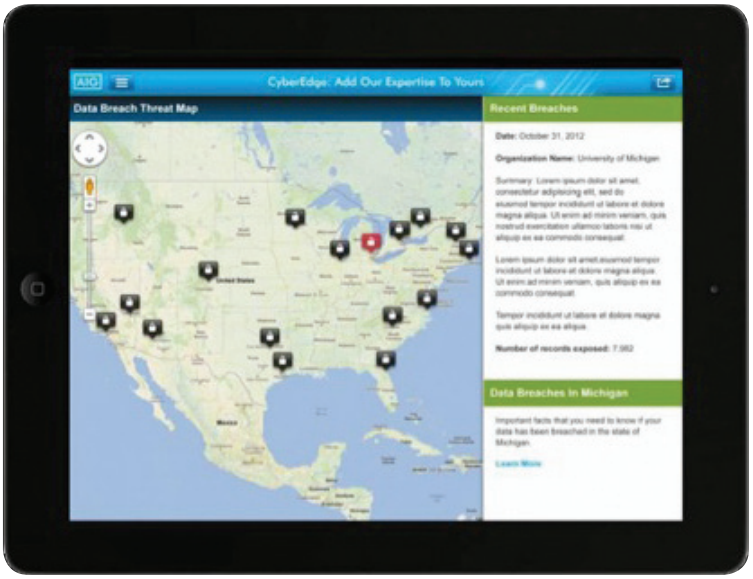
- **Security and privacy liability insurance:** Coverage for third-party claims arising from a failure of the insured's network security or a failure to protect data. Insurance also responds to regulatory actions in connection with a security failure, privacy breach or the failure to disclose a security failure or privacy breach.
- **Event management insurance:** Coverage which responds to a security failure or privacy breach by paying costs of notifications, public relations and other services to assist in managing and mitigating a cyber incident. Forensic investigations, legal consultations and identity monitoring for victims of a breach are all included.
- **Network business interruption insurance:** Coverage which responds to a material interruption of an insured's business operations caused by a network security failure by reimbursing for lost income and operating expenses.
- **Cyber extortion insurance:** Coverage which responds to the threat of intentional security attacks against a company by an outsider attempting to extort money, securities or other valuables. This includes monies paid to end the threat and the cost of an investigation to determine the cause of the threat.

* Refer to the policy for terms, conditions and limitations on coverage.

Risk Management

Companies Affiliated With AIG Offer a Number of Innovative Risk Management Tools Designed to Keep Users Ahead of the Curve

CyberEdge Mobile App
The free CyberEdge Mobile App for iPads combines the latest cyber news, opinion and risk analysis with real-time updates on country-wide data breaches, putting cyber information at user's fingertips. The app is available for free on the App Store.



User benefits:

- All the latest cyber news from industry-leading news providers
- Up-to-the-minute information on country-wide data breaches
- An extensive database of cyber resources
- Risk analysis tools to help determine potential liability costs
- Information on CyberEdge and contact details

CyberEdge RiskTool

CyberEdge RiskTool is a single, web-based platform that helps clients streamline the risk management process. The platform's content is highly customizable and can be tailored specifically to meet the user's needs. Examples include assisting in a compliance initiative, educating employees on regulatory requirements or training staff on security protocols to help prevent human error from causing future breaches.

Risk management modules include, but are not limited to:

- **Security**: Provides an interface where an IT department can manage a company's shunning technology, AutoShun®, which blocks known cyber criminals from communicating with a company's network.
- **Training**: Includes pre-populated training content and tests with an online assignment engine to deploy employee training and awareness with the click of a mouse.
- **Compliance**: Comes pre-loaded with security policy templates that can be accepted or modified to fit each company's needs. If strong corporate security policy is already in place, existing policies can be uploaded and tasked to employees or third-party vendors to confirm receipt and acceptance.

Cyber and Data Security Risks and the Real Estate Industry

AutoShun®

AutoShun® complements the most powerful first line of defense in preventing cyber threats — a company's own IT system. The hardware device is powered by leading edge intelligence that isolates damaging internet source areas, keeping them out of a company's network. With millions of known "bad" actors constantly updated on the current shun list, AutoShun® identifies and blocks the largest sources for malware, crimeware and fraud.

How AutoShun® works:

- AutoShun® stops an attack by bidirectionally blocking communications to known "bad" IP addresses.
- The shunning capability disrupts the infected computers' ability to communicate back to the command and control servers, eliminating the botnet's ability to carry out its criminal functions.
- The attack information is sent to the accompanying CyberEdge RiskTool account, which updates information on "bad" IP addresses in real time.

Conclusion

Real estate firms, regardless of size, no longer have the luxury of believing they are immune from cyber attacks or the predations of cyber criminals. Awareness of this increasing risk and preparedness in its face is paramount. Real estate firms can now add AIG's expertise to theirs through CyberEdge®, a comprehensive risk management solution for cyber insurance.

Footnotes

1. Identity Theft Resource Center 2013
2. *2012 Cost of Cyber Crime Study: U.S.*, Ponemon Institute
3. *Cybercrime insurance Takes off as Providers Target Smaller Businesses*, Wall Street Journal; January 25, 2013
4. *Cybercrooks Target Vulnerable Small Businesses*, February 28, 2011
5. *The Everything Landlording Book*, Judy Tremore with Deborah Boersma, Zondervan 2009
6. *SMBs Unprepared For Security Breaches*, March 11, 2013
7. *In Defense of Data; Views from the Frontline of Data Protection;* Data Breach Trends and Stats In Defense of Data, 2013
8. *Bad Outsourcing Decisions cause 63 percent of data breaches.* Sharedserviceslink.com; February 2013
9. Trustwave 2013 Global Security Report
10. *In Defense of Data; Views from the Frontline of Data Protection;* Id.
11. Id.
12. Id.
13. Ben DiPietro, DowJones.com; January 30, 2013

Bring on tomorrow

AIG Property Casualty
175 Water Street, New York, NY 10038
multinational@aig.com | www.aig.com