Hackers seek personal data too: Here's why and what to do

Many people think cyber criminals are after financial data only or at least primarily, but that's no longer the case. Hackers are seeking personal data on as many victims as possible, data they will sell to the highest bidder or to already established clients.

Personal data is almost like currency in terms of its value to merchants worldwide. They use it to market just about everything directly to potential customers- via email, via links that pop up in Facebook and other social media outlets, via regular mailers and in every manner of media advertisements. The use of personal data in marketing is pervasive and very sophisticated, with marketing analytics figuring out how you buy, where you buy, when you travel, what you watch, how much you make, where you live and eat, and whom you know, among a thousand other things.

Multi-family residential complexes typically hold personal data on their residents, possibly including contact information, ages, emergency contacts, financial information, and automobile details. All of that is worth money to cyber burglars, and that makes your organization susceptible to the costly ramifications of a cyber-breach. Expenses often include the cost of notification of all victims; the cost to protect and/or restore credit or other business, financial or private holdings of those harmed in the breach if your group is found liable; attorneys' fees; public relations fees; and possibly fines or other sanctions regulators or courts might impose.

Not all data breaches occur because of malicious outsiders. Sometimes insiders sell such data, either because they are disgruntled employees or because they've been lured by money. It depends on the details of a cyber-breach, but there are multiple layers of protection your management needs to consider.

Tracking and limiting access to data stores is first on the list of security. Second is monitoring activity into and out of your databases. Third is marking that activity so, if a breach occurs, it may be possible to trace the activity to a computer. Fourth is making sure employees who have access to data are trustworthy. And fifth is insuring against both cyber breaches and internal crime. Your insurance agent should be able to help you find a cyber-security policy and a fidelity policy that work together to help protect you financially in the event resident data is stolen or accidentally transmitted. If you use a third party for payments or any other service that requires personal data of residents, check into their storage and protection methods also since you might be held responsible if their systems are compromised. The same holds true if you are sub-contracting your data security to a cyber-firm. They need to prove they have the appropriate protection and insurance in case of a breach.

Investigate all employees before hiring them and invest in training for your staff so errors are minimized. Human failure accounts for more compromised data than cyber hacking and can lead to losses even in apartments and condos that have solid online protection. Take steps to keep sensitive data stored on hardware that isn't linked to the same systems that are used for online shopping or social media.

When you consider your insurance choices, also look into legal services and public relations services that are offered alongside the policy. Some providers give access to hotlines and media relations specialists that can make the aftermath of a data breach easier to deal with. You also need to be aware of the law in your state regarding cyber breaches. Each state has its own set of statutes that could expose you to costly penalties.

Posted by **Global Administrator** on 5/6/2014 1:27:46 PM