
20
1
18
5
12
9
14
11
8
16
7
19
3
17
2

Lose the Bullseye

Personal data protection by apartment owners is rising on the list of the industry's greatest risk management topics.

BY FRANK MAUCK

Viewed through the lens of rental housing operations, Target Corporation's recent failure to adequately protect sensitive consumer information underscores the fact that although a necessity, the collection of residents' personal data is now an even greater liability.

Even the seemingly innocent task of making a photocopy of a prospective resident's driver's license can put data at risk, potentially leaving apartment owners and management companies liable, facing costly legal bills and settlements.

The multifamily housing industry must direct more attention at personal data protection, given the recent and continual onslaught of computer hackers looking to steal personal information, whether through credit card transactions or from companies' information technology systems.

While technology is creating new and better safeguards against such crimes, hackers have shown they often are able to stay one step ahead.

In response, apartment companies must familiarize themselves with the state-specific responsibilities they carry for preservation of this data, based on their communities' locations. They must have plans and protocols in place to help identify and deal with breaches that onsite and corporate staff members know, understand and execute.

These efforts are in the spirit of both protecting their residents, the companies' reputations and against lawsuits, says Brian Finch, Partner at Washington, D.C.-based Dickstein Shapiro LLP, a nationally recognized leader in dozens of practice areas including addressing and mitigating the complex threats associated with privacy, data breach and computer technology risks.

"First thing's first: Understand what it is you are collecting and storing," Finch says. "It's so easy to [steal data]."

Consider the volume of highly sensitive personal information swirling around at the community level: Background checks, credit reports, income statements, social security numbers—it's a data bonanza that needs to be protected from any and all "black hats" looking to take part in the field day.

Even in the case of the office copier: The machine often has a hard drive, on which a digital copy is stored of every document scanned. That same photocopier is

connected to your network and therefore considered "inbounds" to any enterprising hacker, Finch says.

Data Breach Plan Creation

Don't have a data breach plan? Better develop one quick, Finch says. Experts from the FBI and other security organizations have warned that the consequences of the Target breach have only just begun, and continue to implore the general public's vigilance in credit report monitoring.

For those in need, Finch offers several considerations when developing such a plan. Before doing anything else, he advises conducting a risk and vulnerability assessment, as you cannot protect what you don't know you have.

Second, develop a comprehensive understanding of the IT system as a whole. Firewalls and antivirus software are just the tip of the iceberg here—consider all the variables in play: Mobile device policies, especially if the company is BYOD (Bring Your Own Device); whether data on company laptops is encrypted; whether computers accessing data (internally and through the web) are required to have security software; whether passwords are changed regularly; the type of access third-parties have and whether that access is revoked upon completion of system use; identifying control systems in place for third-parties; and, importantly, assured destruction of data where required.

Just to name a few.

Finally, a remediation strategy and insurance review round out the beginnings of a comprehensive solution in guarding against unwanted systems intrusion.

Equally important is gaining understanding of the company's obligations at the state government level. Finch says an organization's responsibilities can vary widely, based on the state. Owners and management companies may face multiple sets of obligations based on such far-flung variables as their residents themselves and third-party providers doing business in other jurisdictions.

Lawsuits are being filed against companies, including recent headline-grabber retailer Target, for violating state-specific obligations in regard to consumer data protection.

To date, seven banks have filed class-action suits against Target, contending the company failed its duty to safeguard its customers' data. Of course, as referenced earlier, dozens of the store's customers are quite literally following suit. The company will continue to operate in the shadow of further litigation; expected losses are generously estimated to end up totaling in the hundreds of millions of dollars.

To wit, Target faces one lawsuit in Minnesota alleging it broke state law by taking too much time to alert its customers of the theft. A Pennsylvania-based credit union is bringing a separate case in Minnesota for violating the state's 48-hour limit on maintaining a customer's account information. And it faces yet another suit in California by a customer claiming both negligence and invasion of privacy.

In 2007, TJX, another of many national retailers that have suffered a significant breach, paid a $40 million settlement to financial institutions who filed similar claims based on the company's exposure of 45.6 million of its customers' credit cards—though it's reported that only 15 million were actually at risk based on the fact that the other 30 million or so had expiration dates that had already passed.

The violation ultimately led to TJX paying a $168 million settlement and legal and regulatory fees.

If an owner/operator suspects any kind of digital trespass, Finch says the first course of action is to implement your data breach plan based on the above-mentioned guidelines. Affected residents and other stakeholders should be notified in a timely fashion. It is incumbent on the company to determine the extent of the breach (and ensuring that it is, in fact, over) before moving on to the remediation and forensic phases—essentially asking, "What's been taken and how do we now remove that risk."

So please consider this a public service announcement. A warning shot in a brave new world where such exhortations come few and far between: Don't be a Target.

Frank Mauck is NAA Manager of Communications, reachable at frank@naahq.org.