THE VANTAGE

grace hill

ISSUE NO.
08
DECEMBER 2018
BROUGHT TO YOU BY GRACE HILL and HSB

HAYNSWORTH
SINKLER BOYD

Property Management Cybersecurity Threats

Marriott Hotels learned in recent weeks of a massive data breach of its customer data. Specifically, the breach involved theft of personal information belonging to up to 500 million customers. Marriott is currently dealing with the public fallout, government investigations and legal ramifications. This is the latest in a long string of data breaches in recent years that have wrecked companies in the United States.

Housing providers collect an extraordinary amount of information from applicants and residents. Just think about a lease application – name, address, social security number and employment history, just to name a few. Believe it or not, this information, known as personally identifiable information (PII), is extremely valuable to hackers.

A security breach where this information is compromised can create serious liability for your organization. In recent years, we have seen large government fines and civil suit settlements for security breach cases. Moreover, the public relations fallout from a breach is often the most damaging aspect. This issue of The Vantage provides some examples of the threat within the property management industry and actions that should be taken to mitigate the risk.

Common Misconceptions

The National Multifamily Housing Council (NMHC) and the National Apartment Association (NAA) recommend that multifamily companies operate under the assumption that a cyberattack is inevitable. Yet, the reality is that many housing providers are not prepared. This lack of preparedness seems to be driven by two misconceptions: the business is too small to be targeted by hackers and the data property management companies have is not valuable to hackers. [1]

To dispel the first misconception, here are a few statistics:

71
percent
of cyberattacks take place in companies with **fewer than 100 employees.**

Each victimized company lost over
5,000
individual records,
spent an average of
$880,000
dealing with the problem, and incurred
$955,000
in damages.

55
percent
of businesses attacked between mid-2015 to mid-2016 were **small to medium-sized businesses**.

Six out of **ten** small companies go out of business within six months of a cyberattack [2]

There are a few reasons that cyberattacks are threatening small businesses. First and foremost, smaller companies are less likely to have information technology (IT) and/or security experts on staff to monitor threats and fend off breaches. Thus, deliberate attackers may find these organizations easier to compromise. In addition, housing providers often handle large sums of money and collect personally identifiable information (PII), making the housing industry even more attractive to potential hackers.

However, it is important to note that "malicious hackers" make up a little less than half of all data breaches in small businesses. [3] This means the other half of all data breaches are a result of negligence on the part of employees or third-party vendors. Training employees regarding cybersecurity is key to preventing many security incidents in your organization.

PII is particularly important to understand. Phone numbers, email addresses and billing addresses are the PII digital currency that is in high demand. This type of data is sold between hackers on the "dark web," the digital black market for stolen identities, fake passports, and much more. [4] If a breach occurs in your company, everyone whose information is stored in your databases is exposed to a great deal of risk—and you're exposed to a tremendous amount of liability.

Six out of ten small companies go out of business within six months of a cyberattack.

Potential Consequences

The fallout from a breach – regardless of whether the breach was due to a careless employee or a malicious hacker – can put an organization out of business. One area of exposure is from government fines. State and federal statutes protect consumers from data breaches, and those laws often provide for governments to issue fines against organizations found to be culpable in some manner with the breach. This culpability could take the form of failing to adequately train your employees or implement procedural safeguards. In 2017, Hilton Hotels agreed to pay $700,000 and improve security procedures to settle an investigation into data breaches in which over 350,000 credit card numbers were exposed. Officials found that Hilton had not followed payment-card security standards, did not have reasonable data security and failed to inform affected customers of the data breach in a timely fashion.

In addition to government fines, individual residents and/or applicants could sue your organization if their personal information is compromised. Class-action lawsuits are common in this scenario and the legal fees involved can be tremendous. For instance, Target spent approximately $203 million on legal fees after a 2013 breach.

In 2017, Hilton Hotels agreed to pay $700,000 and improve security procedures to settle an investigation into data breaches in which over 350,000 credit card numbers were exposed.

Precautions Property Managers Can Take Right Now to Prevent Cybercrimes

Below are a few simple, actionable procedures that property managers can put in place to protect the business, owners and residents.

Training

Many of the costliest data breaches occur due to human error and negligence. For instance, clicking on a suspicious email or leaving a computer open at a Starbucks. Properly training your workers is going to be your organization's first line of defense. Employees should understand the threat and know the company's reporting procedures in the event there is a breach or threat. Training will also help reduce potential government fines by showing good faith compliance.

Policies and Procedures

Establish internal protocols for data security that include the following:

- **Require employees to make strong passwords and create two-factor password authentication.** Verizon found that 81% of hacking-related breaches were caused by stolen or weak passwords.[5] Use different passwords for each business and personal account, make passwords strong by never using sensitive information, like names and birthdays, and never use simple words like "password" or consecutive keys like "12345."

- **Install Antivirus, Anti-spyware and Firewall Software - all three of these applications protect your systems from attack.** Antivirus and anti-spyware apps scan for viruses on websites and in email and warn you when they find one. Firewall software is designed to block unauthorized access while permitting outward communication. Finally, update this software or apps whenever a new update is available, as updates repair susceptibilities that hackers can exploit.

- **Back-up data.** Ransomware is now one of the most popular types of attacks. Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Businesses have big problems if the hackers are blocking access to any property management system, but if the hacker is holding data that was already backed-up pursuant to policy, the organization should be in good shape.
- **Have an incident response plan.** Housing providers are advised to create an incident response plan in the event that a breach does occur. The plan should address issues such as who is in charge of communicating with the media, who will notify legal and insurance and who will lead the internal team to secure the information that has been compromised.

Hiring

Hiring experienced IT professionals, specifically with experience with data security, is an important step to protecting PII. Moreover, consider running background checks on potential hires (if legal in your jurisdiction) to make sure that you are not hiring anyone with theft or questionable issues in their past employment. If your current staff does not have the adequate IT or security systems experience, consider hiring a consultant or third party to provide those services to your organization. However, be sure to use reputable vendors for such work and heed the information on contracts below.

Insurance

Housing providers should make sure they have insurance coverage for security breaches. Coverage may not be provided by your normal commercial general liability insurance policies. Insurance companies now offer specific coverage for these situations.

Contracts

Housing providers should work with legal counsel to review contracts with vendors and third-party service providers. Contracts should require that vendors comply with their security requirements, as well as contain indemnification clauses in the event of a breach. In addition, non-disclosure agreements should be entered into with employees and independent contractors.

Proactively Protect Your Data

You can further strengthen your property management company's risk posture by being strategic about the data you own, use, share and store. For instance, carefully select who is allowed to access sensitive data, make sure all data is encrypted, avoid hanging onto records you don't need and store important data securely off-site.

81% of hacking-related breaches were caused by stolen or weak passwords

Conclusion

Cybersecurity breaches are a serious threat. Make sure you are taking proactive steps to protect your data and prepare for any potential attack. Proper training, security protocols and legal counsel are key to reducing risk.

Cybersecurity Training Is Your First Line of Defense

To be effective, cybersecurity training needs to address the unique security risks of your industry – and prepare employees in all roles to tackle them. Most security risks in the multifamily industry fall outside the "IT specialists" area of responsibility, which is why all employees need to understand and help manage cybersecurity. Grace Hill's new Cybersecurity for Multifamily elective course series is designed for multifamily employees in non-technical roles. It breaks down the risk of cybercrime and equips all property management professionals with practical strategies to help prepare for and prevent cyberattacks. **See for yourself how effectively the course helps multifamily companies reduce risk.**

Notes

[1] Robin Young, Cybersecurity 101: What Property Managers & Landlords Need to Know – Part 1, available at https://www.buildium.com/blog/cybersecurity-for-property-managers-1/

[2] Id.

[3] Matt Mansfield, Cyber Security Statistics: Numbers Small Businesses Need to Know, available at https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

[4] See Young, supra note 1.

[5] Verizon's 2017 Data Breach Investigations Report, available at https://www.verizonenterprise.com/resources/reports/2017_dbir_en_xg.pdf

grace hill

Grace Hill partners with clients to protect their multifamily business and prepare their employees to succeed. Armed with the industry's most robust training catalog, comprehensive customer support and innovative solutions to complex business problems, Grace Hill clients are able to provide a high standard of service - for residents and employees. Let's move forward together.

HAYNSWORTH
SINKLER BOYD

Haynsworth Sinkler Boyd, P.A. advises multifamily housing clients on compliance and business matters, including FHA, ADA, state and local fair housing laws, and employment matters in those states where our attorneys are licensed to practice. For more information on how Haynsworth Sinkler Boyd may help your business, contact shareholders Frank Davis, One N Main St., Greenville, SC 29601, (fdavis@hsblawfirm.com) or Andrea Brisbin, 134 Meeting St., Charleston, SC 29401, (abrisbin@hsblawfirm.com) and visit hsblawfirm.com.

gh

Grace Hill
15 S Main St, Suite 500, Greenville, SC 29601
866-472-2344
www.gracehill.com