Identity and cybersecurity criminals want what you have.

**Are you protected?**

# ARE YOU SITTING ON A CYBER SECURITY BOMBSHELL?

BY JOSEPH DOBRIAN

**CYBERSECURITY IS A MAJOR ISSUE IN MANY INDUSTRIES THESE DAYS:** particularly in financial services, defense, medicine, journalism and social media. It's also an issue in commercial real estate, but not many people in the industry are aware of the hazards involved in a cybersecurity breach.

Property managers, in particular, tend to be uninformed of this issue. They remain so at their peril.

Recent high-profile hacks of corporations such as Home Depot, JP Morgan Chase and Target have raised awareness of cybersecurity issues among real estate professionals. Still, as an industry, property management needs to broaden its knowledge and up its game when it comes to protecting data.

## PROTECT YOUR RESIDENTS' PII

It could come as a surprise to some property managers, when they consider the situation, how much vulnerable data they have control of. Not only do they have various accounting functions and maintenance histories on file: They also, typically, have an extraordinary amount of personally identifiable information (PII) on their tenants—especially if they're managing a residential property. A resourceful hacker could use a property manager's database to steal identities, commit extortion and destroy reputations.

Paul Kastes, CPM, LCAM, who heads Principals Management Group in St. Petersburg, Fla., reported that the issues a property manager will face, with regard to cybersecurity, will depend largely on the size of the portfolio, the number and type of tenants involved and the methods of data storage. Bigger management companies run bigger cyberrisks; the vast majority of smaller companies, he said, are still on paper or use a combination of computers and paper.

"In the field," he said, "the biggest issue is protecting the information that we keep on residents and potential residents. We have Social Security numbers on these folks: That's valuable to people who want to steal it. If you get a person's social, you can do just about anything. You have their name, address, where they used to live and their driver's license numbers: you can be another person in five minutes. Protection of the residents' Personally Identifiable Information (PII) is a huge concern.

"You have to hire the right people, to ensure that the information is protected. Many people in our industry aren't computer savvy. They need to know that if you open the wrong e-mail you could be in trouble. As we go on, with increased reliance on internet and computers, this issue will get worse, and your firewalls are only as good as your people. You have to monitor and supervise them."

Background checks on your employees are a must, Kastes said, but managers still have to be constantly vigilant, because the greatest threat comes from within the company.

"That threat is less for a smaller company that has a sophisticated IT department," he pointed out. "For a smaller manager it comes down to supervision and staffing."

## DATA AT REST ARE DATA AT RISK

"Identity theft is the big issue," said David Lingenfelter, Information Security Officer at Fiberlink, an IBM company.

"Mobile and cyber security are very closely related; everyone's working from their mobile device now, and if you leave your phone behind someplace, you've exposed a lot of data. Data aren't managed anymore; everything is out there on a cloud, not going back to a centralized corporate server.

Daniel Gonzalez, CEO of D.A.D. Protection Services, provides advanced security advice and programs for Class-A high-rise facilities and industrial warehouses. Gonzalez said the most vulnerable data are rental applications and credit reports, the abuse of which could damage not just the individual victim, but the economy overall. And the risk, he said, lies not only in cyberspace.

"Never leave paperwork lying around, even in locked files," he urged. "Put it on a flash drive, password protected, in a locked drawer. Only the owner, and/or the owner's secretary, should have the password.

"Have your security people check trash cans and empty boxes, and have a disposal protocol for paperwork, to alleviate hands-on theft. You'll never be able to keep up with the technology; that's why you should keep data on a flashdrive and only use it off your flashdrive."

Jay Shobe, vice president of technology at Yardi, explained that data in motion are largely protected from hackers because they're encrypted. Data at rest are data at risk, he warned.

"You have to have encryption embedded in the database," he advised. "You can leverage your database to do your encryption for you; some changes must be implemented to the software application and that isn't always easy. You should also think about improving the security of the corporate network. You have to have the right firewalls and your user credentials must be protected. A breach usually is caused by one person's password being compromised. One thing clients can do is implement 'single sign-on,' which ties many apps to an active directory, instead of a manager accessing the rent portal, accounting system, etc., with four or five passwords."

Security awareness training for your staff is a must, said Shobe, as is monitoring—often via surprise tests.

"Clicking on an attachment in an e-mail is a simple thing but can be devastating," he said. "If you click on it, the intruder's in, and can poke around. You can send suspicious-looking e-mails to your employees to test them. If they click on an attachment, a pop up will say, 'OOPS! You're going to be automatically enrolled in an internet safety course!' It's a teachable moment, a way to give the employee a slap on the hand and heighten awareness of the problem."

Data loss prevention is another problem, said Shobe: He urges managers to monitor egress channels such as e-mail and removable media. ■

## INSURERS OFFER HELP IN FIGHTING CYBERCRIME

Insurance companies hate to pay—so they're helping real estate owners and managers to protect themselves from cybersecurity breaches. According to Kevin Smith, CPCU, ARM, vice president of the real estate division at The Graham Company (a Philadelphia-based insurance broker), property/casualty insurance policies were never intended to provide coverage for liability and first-party notification expenses resulting from the disclosure of personally identifiable or confidential corporate information. In fact, he said, insurance carriers have started adding exclusionary endorsements to ensure that their policy language doesn't provide coverage for these potential claims. In response to the gap in coverage, insurance companies have developed cyber liability policies. However, he warned, many off-the-shelf cyber policies don't fully protect the client.

"Some cyber policies don't provide coverage for breaches of protected information in paper files, or claims brought by government or regulators, or if a commercial property company fails to encrypt data," he warned.

"We can cover breach or loss of data whether it's on a computer or on paper," he said. "What you'd pay for, say, a million-dollar limit, might be based on the number of records you have, what protection you have in place with your security systems and what you have to ward off breaches. These policies aren't that expensive; we're still learning how to price them. They usually require some sort of deductible or retention. The underwriters want to be sure your data is encrypted, that access policies are in place."

Typically, said Smith, the costs of a breach are associated with notification. Liability is rare; seldom does a breach cause real harm that would incur a judgment against a property owner.

"But don't overlook additional coverage," he urged. "Discuss it with your insurance people and your IT people to make sure you're protected. You want to protect your buildings—but you also want to protect your company from liability in case of data loss."

## 'INTERNET OF THINGS' POSES NEW THREAT

It's not just office computers and mobile devices that might be prey for cybercriminals. According to Nigel Somerville, MBE, MC, managing director of risk management at Source8 (London), the "Internet of Things" (IoT) has created many new opportunities for nefarious hackers, and the dangers are growing exponentially.

The connection of physical objects to the Internet and to each other through small, embedded sensors, supported by wired and wireless technologies, has created an ecosystem of "ubiquitous computing," Somerville explained. Universal connectivity means universal vulnerability, and increased threat.

"The IoT not only increases the real estate industry's overall vulnerability to cyber-attack, it also fundamentally alters the nature of the threat," Somerville warned. "It's no longer restricted to the lone hacker or the disgruntled student. It includes well-organized and funded networks of cybercriminals and terrorists."

The areas of real estate industry that stand to benefit most from the IoT, Somerville said, are also the most vulnerable: Building Management Systems (BMS) and Energy Management Systems (EMS). These systems represent the brain and nerves of modern real estate infrastructure and will be subject to increased risk of attack as sensors, systems and networks become increasingly connected.

"Not only will such networks present thousands of potential access points, but also many of them will be parts of systems for which security has never been considered a major concern before," he said. "Since IoT will play a crucial role in Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) control systems and Automatic Identification Systems (AIS), the lack of a secure foundation will represent a systemic vulnerability to all levels of modern corporate infrastructure. On top of that, BMS and EMS systems also suffer from common basic weaknesses including poor password protection, unmonitored access points and rudimentary software."

Attacks could therefore directly impact workplaces, individuals and business operations. Businesses could be temporarily deprived of control over their own management systems, or be locked out completely.

"We can expect to see new forms of blackmailing and extortion schemes, such as ransomware for data theft, smart machines, smart offices or business BMS," Somerville concluded. "Public power utilities, critical national infrastructure, a city's supply distribution networks or the banking system will all become potential targets of attack and may involve real estate and infrastructure."

---

JOSEPH DOBRIAN IS A CONTRIBUTING WRITER FOR *JPM*®. IF YOU HAVE QUESTIONS REGARDING THIS ARTICLE OR YOU ARE AN IREM MEMBER INTERESTED IN WRITING FOR *JPM*®, PLEASE E-MAIL MARIANA TOSCAS AT ***MTOSCAS@IREM.ORG.***