



WHO'S MINDING YOUR ASSOCIATION'S TECHNOLOGY?

Protecting Your Hardware and Data
While Ensuring Exceptional Service

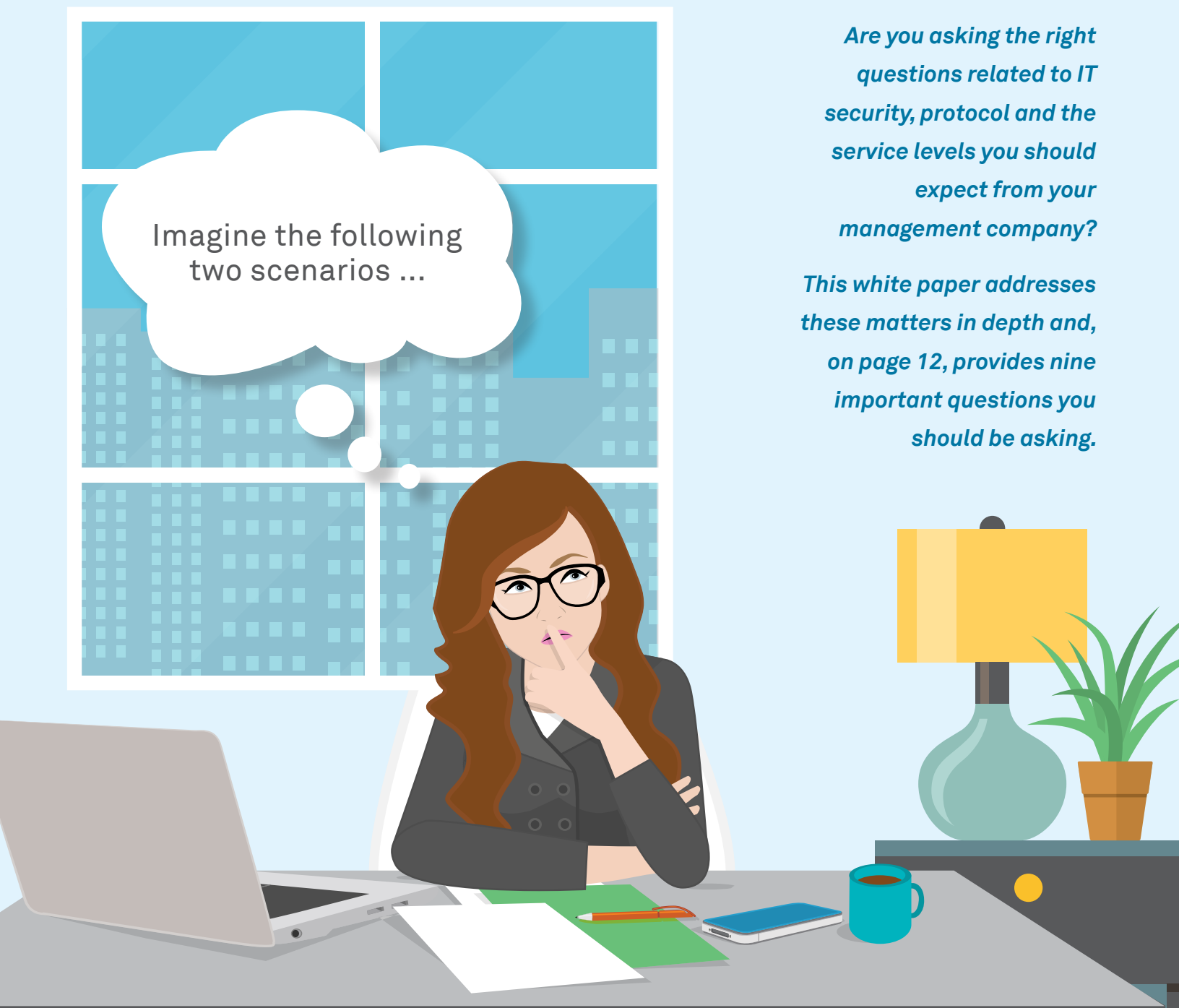


FirstService
RESIDENTIAL

INTRODUCTION

By Tony Joseph, PMP

Vice President of Information Technology, FirstService Residential



Imagine the following
two scenarios ...

Are you asking the right questions related to IT security, protocol and the service levels you should expect from your management company?

This white paper addresses these matters in depth and, on page 12, provides nine important questions you should be asking.

SCENARIO 1

As board members for an association in California that has been self-managed or that has been partnering with a management firm for a considerable amount of time, you've been comfortable with the technology decisions made so far. Up until now, you have outsourced your technology needs to a local vendor. In addition to hosting your financial software, this company has been providing tech support at a great price for several years.

One day, a member of your onsite staff calls the vendor with a computer issue, only to find out that the company has gone out of business. Without giving your board any notice, the owner accepted an offer to work for the large company that created your financial software. Your association is suddenly left with no tech support. Even worse, you have lost all of your community's data, since none of it was transferred to you before the vendor went out of business. Neither your board members nor the new community management company that you have hired is able to track down the owner.

To make matters worse, your new association management company discovers that your security software is out of date and that several of your staff's computers are infected with malware. These same computers are used to access, input and process your payments and to store homeowners' financial details. They have also been used to process homeowner transactions, such as security deposits to reserve the clubhouse and payments for new gate remotes or café purchases. Unbeknownst to you, this malware has been collecting and supplying your financial, and perhaps even credit card data, to a nefarious third party. Perhaps you've had a fraud alert on that same credit card or received a suspicious email regarding your recent payment. Coincidence?



We would all like to believe that these scenarios could never happen to us, but both of these stories are based on real events.

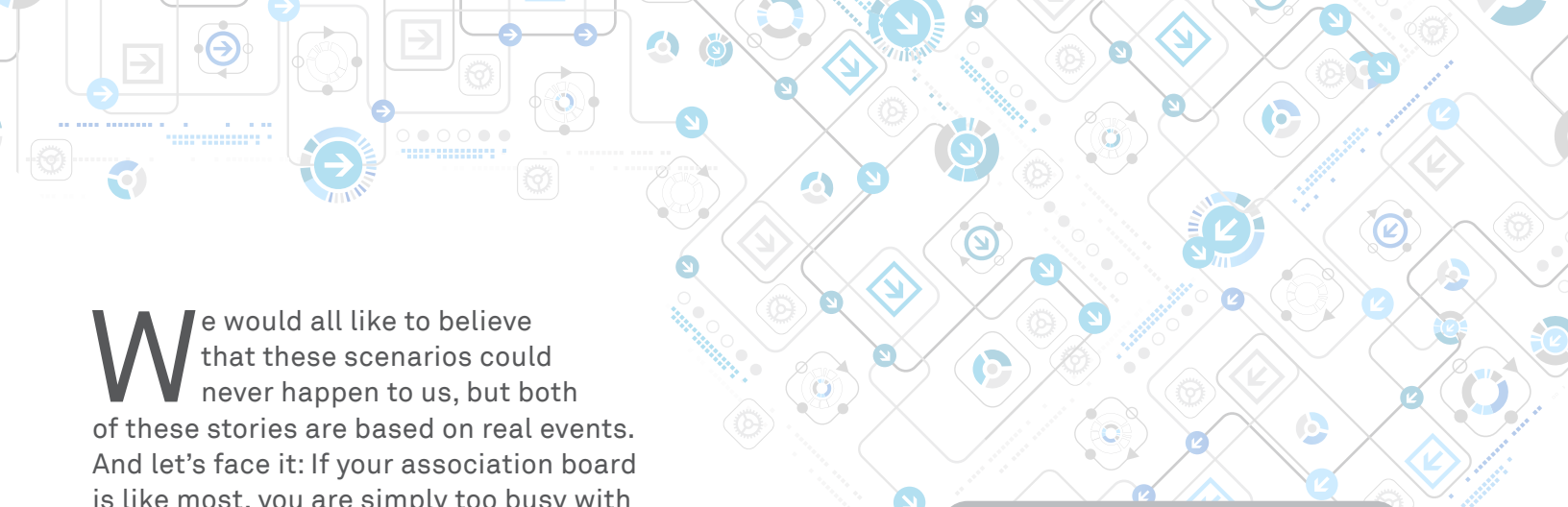


SCENARIO 2

Your board has put a lot of trust in your general manager (GM). In addition to addressing board requests, managing residents' expectations and overseeing onsite staff, your GM has been supporting all of your technology singlehandedly. Although not a technology expert, the GM “knows enough” to get by and save you some money. Among the tech support tasks that the GM has been handling are the email accounts for onsite staff and board members that are tied into your website domain. It's been seamless on your end. However, given the GM's limited technology knowledge, how do you know whether your email accounts are safe from hackers, whether you are getting all the latest security and software updates and whether your computers are receiving needed maintenance?

The GM has also been responsible for hiring vendors to provide services, for processing their invoices for payment and for reporting to you on the budget each month. In your last board meeting, you happened to notice that JT Property Services had been consistently billing you each month and that payments had been going out to them. You don't recall seeing a vendor onsite that often, and you're not even sure what they do. You and the other board members are wondering about the legitimacy of those invoices to JT Property Services. You decide to dig a little deeper, but discover that you can't access your GM's email account because you don't have administrative rights. The GM is the sole person with rights to all the data sitting on your computers. With so much control in the hands of that one person, how can you find out if your GM has been embezzling money from your community and for how long? And who in the world is JT Property Services?





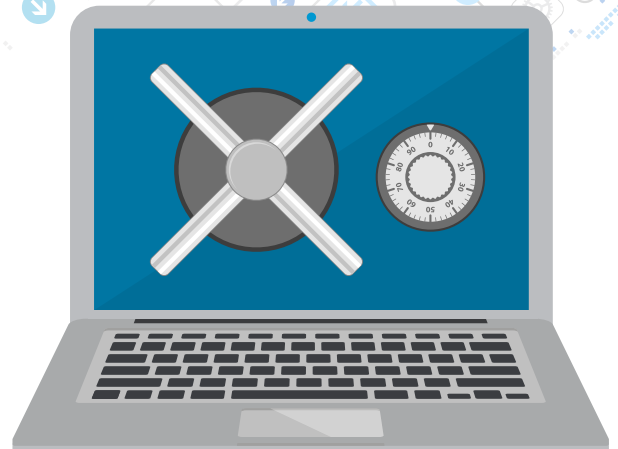
We would all like to believe that these scenarios could never happen to us, but both of these stories are based on real events. And let's face it: If your association board is like most, you are simply too busy with other issues to give much thought to protecting and maintaining your information technology (IT). Sure, you know that malware, hardware issues and data losses could potentially wreak havoc on your association's ability to function effectively, but it's just not your highest priority given all the other matters you have to manage.

So you may have found yourself entrusting your community's technology support to a tech-savvy homeowner, friend or self-employed computer consultant who claims to know the best IT approach for your community. However, bringing in such outside "experts" isn't usually the best solution. Ask yourself these questions:

- ▶ How well have you vetted their technology understanding and background? (For that matter, how well-versed are you in doing that type of vetting?)
- ▶ Do you know where they store your data and how secure it is?
- ▶ What investments have they made to ensure that hackers can't get in and steal your financial information?
- ▶ Are you certain that they don't carelessly leave information sitting on office computers for anyone to see?
- ▶ How confident are you that they don't store your data on shared or cloud-based servers with data from other companies or individuals unrelated to your association?

Besides these important concerns, a small vendor may not always have someone available to address your issues in a timely manner or be capable of making the technology investments necessary to ensure that your data is secure. In addition, they won't be familiar with your community's needs or the business of running an association. Even if you work with a professional community management company, there is no certainty that the company has any more technology expertise than you do. So what's the solution?

This paper looks at why it has become more crucial than ever for associations to prioritize IT management. It examines the benefits of hiring a community management company with in-house IT expertise and describes the best way to evaluate a management company's IT capabilities.



IT MANAGEMENT: WHAT'S IT GOT TO DO WITH ASSOCIATIONS?

Your association relies heavily on IT, even if you might not give it a lot of thought. Your front desk and other onsite staff use technology to check in guests and receive and track packages. Your residents use community websites to pay assessment fees and read association newsletters. And your boards use email to communicate with residents and maintain online databases of resident information. But how safe and dependable is your technology? Are you using reliable hardware and software, or are they old and outdated? How would you function if your system suddenly went down, if the data became corrupted or if you became the victim of a cyber attack? Would you be back up and running quickly? Would you be able to recover all of your critical information?

Even if no one on your association board is a technology whiz, these are questions for which you need the right answers in order to protect the information entrusted to you and keep your systems running reliably. Ignoring IT management will only set you up for big problems down the road.

There are five important aspects of IT management that every association needs to think about. These are cyber attacks, hardware requirements, software requirements, equipment repairs, and data backup and storage.

1. CYBER ATTACKS

A large part of managing an organization's technology these days revolves around protecting personal information. We've all heard about hackers who have managed to access the data of large organizations like Yahoo, Target and the Democratic National Committee. These cyber attacks make big news. However, what we don't hear much about are the attacks aimed at small businesses. Take spear phishing, for example, whereby an infected document is attached to an email. You may be surprised to learn that, according to the 2016 Symantec Internet Security Threat Report, 43 percent of all spear-phishing attacks in 2015 targeted small businesses, compared to only 18 percent in 2011.



In California, which has led the way in creating legislation regarding data breach notification, businesses and state agencies must report any breach that impacts more than 500 Californians to the state Attorney General. Small businesses accounted for 15 percent of the breaches reported in 2015. (This number, of course, does not reflect the smaller-scale breaches that did not need to be reported.)

What makes small businesses an easy target for hackers is that they often store personally identifiable information just like larger organizations do, but they are much more vulnerable because they lack the investment and resources to protect that data. Furthermore, many small business owners continue to believe that they are at less risk than their larger counterparts. Even among those that are concerned about cyber threats, 51 percent still do not budget any money to protect their data.

So what do these statistics have to do with your community association? As a nonprofit corporation, your association is a small business, too. Plus, from a hacker's viewpoint, your association is a great target. You store some very valuable data online—resident phone numbers, postal and email addresses, Social Security numbers, credit card information and other financial data—and you might not be doing enough to keep it safe. Furthermore, your small business is run by volunteer board members whose time is already stretched thin handling regular association responsibilities. If for-profit businesses can't find the resources to address cyber security, how will you?

2. HARDWARE REQUIREMENTS

Almost as soon as you buy new computers, servers or other hardware for your association, those items depreciate in value and begin a path toward obsolescence. Still, older hardware is more likely to break down, run too slowly or be incompatible with newer software applications.

Leasing equipment is one way you could keep up with emerging technology and avoid large outlays of money. However, you would still incur unexpected maintenance and support costs. Additionally, it may lock you into unfavorable agreements or have limitations that are not in the best interest of your association. It is not always easy to determine which option is most cost-effective and beneficial for your association.

From a hacker's viewpoint, your association is a great target. You store some very valuable data online and you might not be doing enough to keep it safe.



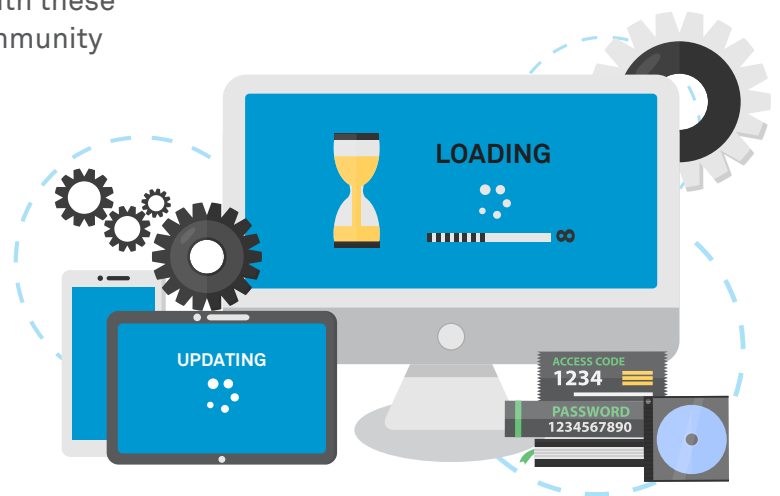
3. SOFTWARE

Associations often depend on off-the-shelf software applications, but tweaking them is frequently necessary to adequately meet your business requirements. Specialized software can address many association needs, but it is not always compatible with other applications and the associated costs may not fit your budget. Most associations are forced to cobble together a variety of disparate products. This results in inefficiencies and manual work, leaving too much room for errors and omissions. Getting the right combination of applications that work well together can be a challenging and costly undertaking.

Busy board members and community managers may also neglect to install the updates that software companies regularly provide. Usually called “service packs” or “patches,” these updates are sometimes designed to enhance the application, fix bugs or add security enhancements. Most of the time, they address vulnerabilities in security, but if you don’t keep up with these system-wide updates, you could be leaving your community open to potential attacks.

How do you know if you have the right software and if it is up to date? Are updates handled by an outside computer vendor, or are you responsible for updating your own software? How soon after an update is announced is it installed at your site? Have you chosen to let the software “update itself” without testing it to ensure that the update doesn’t break something else or adversely impact another reliant system?

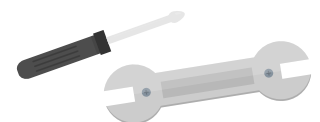
Most associations are forced to cobble together a variety of disparate products. This results in inefficiencies and manual work, leaving too much room for errors and omissions.




4. COMPUTER REPAIRS

Sooner or later, we all experience a malfunction with our computers, routers or other equipment. Having even one computer down can be a real inconvenience, especially if, for example, your onsite staff depends on its system to manage day-to-day business.

Working with an outside vendor puts you entirely at the vendor’s mercy. You don’t know how quickly someone will be able to get out to your property to evaluate your problem. You don’t know when you will have your computer back if the vendor has to take it offsite. And you have no way of knowing how many people will have access to residents’ private information, especially if your local vendor has to send the computer to a third party for servicing.



Working with an outside vendor puts you entirely at the vendor’s mercy.



An event such as a lengthy power outage, a natural disaster or a cyber attack could cause your association to lose crucial information—unless your data is properly backed up and stored.



5. DATA BACKUP AND STORAGE

An event such as a lengthy power outage, a natural disaster or a cyber attack could cause your association to lose crucial information—unless your data is properly backed up and stored.

This means that your approach must ensure both safety and reliability. Of course, any backup approach will have very little value if you aren't disciplined about performing your backups often and regularly.

According to a survey conducted by CyberScout, “22 percent [of small business owners] said they weren't sure how to back up their systems and files, or didn't realize the need, or the extent to which data must be secured.” Others assumed that what they were doing was adequate when, in fact, it was leaving their data vulnerable. Additionally, some didn't know how to use the backup once they truly needed it.

For example, if you store your data on a hard drive that you keep onsite, a fire that prevents you from accessing your computers would also prevent you from accessing your backup. A theft could also result in the loss of both your computer and your hard drive. And in the event of a cyber attack, your backup could wind up having the same virus as your computers since malware often hides undetected for a period of time.

Storing your backup on the same server that you use for your association system could prove futile in the event of a ransomware attack (a cyber attack that locks up your system until you pay a ransom). And with a cloud backup solution, your reliability, bandwidth and recovery speed would be highly dependent on the capabilities of your vendor.

THE RIGHT BALANCE: A COMMUNITY MANAGEMENT COMPANY WITH IT EXPERTISE

Communities often opt to hire a technology vendor to address their IT management needs. However, as the previous section demonstrated, some of the issues this could present include the following:

- ▶ A lack of understanding about the needs of your association
- ▶ Slow responsiveness
- ▶ Lack of dedicated service
- ▶ High or “unbudgeted” costs
- ▶ Downtime during offsite hardware repairs
- ▶ Third-party access to your association’s sensitive information



Many associations work with a community management company to handle their ongoing operations and maintenance, enforce their policies and communicate with residents. These companies have an in-depth understanding about the needs of associations and can take the burden of day-to-day operations off board members.

The best management companies will also have a highly skilled team of dedicated IT professionals who can manage your community’s IT needs. Working with an IT team that is part of your management company allows you to benefit from solutions designed specifically for associations. These experts will already be familiar with the requirements of associations and will work hand in hand with the rest of your management team. More importantly, the same company that you have entrusted with your sensitive data will be responsible for maintaining the systems on which that data lives.

The best management companies will also have a highly skilled team of dedicated IT professionals who can manage your community’s IT needs. The same company that you have entrusted with your sensitive data will be responsible for maintaining the systems on which that data lives.

Ideally, you should work with a company that is publicly traded. Public companies must undergo regular financial and internal audits, and these are often accompanied by IT security audits, which serve to determine the effectiveness of their security protocols.



EVALUATING A MANAGEMENT COMPANY'S IT CAPABILITIES

People often fear change, but a small-step approach can help put those fears to rest. Show residents the value of lower-cost, easy-to-implement amenity and service upgrades. Giving residents a taste of what real lifestyle-driven enhancements can achieve, without significantly affecting the association's budget, will make them more open to larger-scale capital improvements down the road.

COMPANY SIZE

Small, local management companies are vulnerable to the same types of cyber attacks as any other small business and often lack the ability and financial investment to provide the level of support your community needs. On the other hand, a large company that has a significant local presence is better positioned to provide you with extensive onsite IT support and the resources to back up that support. It is also much more likely to implement the most sophisticated security measures to protect its systems—and your data—from hackers and other sources of unauthorized access.


Ideally, you should work with a company that is publicly traded. Public companies must undergo regular financial and internal audits, and these are often accompanied by IT security audits, which serve to determine the effectiveness of their security protocols.

IT STAFF

The management company should be able to provide you with a dedicated team of highly trained specialists to evaluate your IT infrastructure and determine the best setup for your association. You also want to know that the IT staff is large enough to adequately provide the level of support you need and address any issues.

RESPONSE TIMES

When one of your computers goes down, time is of the essence. Onsite employees cannot do their jobs if your technology or software problems are not addressed quickly. Without readily available IT support, the staff and homeowners may experience unexpected and unacceptable delays.



Make sure that your data is housed at a data center that is built and maintained according to the highest standards

OWNERSHIP

The community management company needs to be capable of handling all of your equipment repairs, software updates, security requirements and data backups. It should take full responsibility for protecting your data, which means not entrusting it to third-party vendors. In addition, the management company should properly vet any software providers to ensure that they adhere to the highest security standards and that all software works well together.

Although you want the security of your data in the hands of the management company, it's important for your association to retain ownership and control of the actual data. This should go without saying; however, you may want to verify this with the management company beforehand.

IT SERVICE OPTIONS


Many computer issues can be addressed quickly by partnering with IT staff onsite or remotely, so you want to be sure that the management company offers these options. For example, with your permission, a tech expert can access an individual workstation to make updates or change settings. The company should also be capable of providing scheduled and tested updates seamlessly to your entire system. Additionally, you should be able to depend on your IT support to provide current technology at any time to ensure that your operations run smoothly.

DOWNTIME

If a computer needs to be taken offsite for repairs, the management company should be able to provide a temporary replacement quickly so that staff members can continue to perform their duties. Automatic updates should be performed during times that will cause minimal disruption to your staff's regular activities.

DATA STORAGE

Make sure that your data is housed at a data center that is built and maintained according to the highest standards to keep your systems operational and your data secure. Equally important, data backups should be kept off-site at an alternate location to prevent them from being jeopardized.



Are you asking the right questions related to IT security, protocol and the service levels you should expect from your management company?

ASK THE RIGHT QUESTIONS

Here are nine things you should ask your community management company about its IT management approach:

1. What kind of security protocols do you implement for onsite associates and their workstations? How often are those security measures audited and updated?
2. How are software applications accessed and who controls the administration?
3. Do you provide and support hardware?
4. What disaster recovery processes do you have in place in case of a breach or data loss?
5. Where will our data be stored specifically, and will it be housed on servers with data belonging to non-clients?
6. Where will our backup data be stored?
7. Will any third parties have access to our data?
8. Will our association retain ownership and control of the data?
9. How do you ensure that your staff properly handles our data? (Do you have any auditing processes and security policies in place? Do you restrict access? Are duties segregated? What is the vetting process for the vendors you hire for our association?)

THE FIRSTSERVICE RESIDENTIAL DIFFERENCE

From the time an association hires FirstService Residential California to be its community management company, we take on the responsibility for all aspects of the community's IT management. Our highly trained IT professionals know what it takes to meet the needs of associations. They work closely with the entire FirstService Residential management team, as well as with the association's board of directors, to address the unique needs of each client.

Tony Joseph, PMP

Vice President of Information Technology
FirstService Residential

Tony Joseph has been with FirstService Residential since 2014, overseeing IT operations for the central and western United States, along with central and western Canada. Tony leads a team of technology professionals who support, champion and implement operational standards for FirstService Residential offices and for communities that the company manages and staffs. His involvement in creating the company's technology roadmap helps ensure operational excellence, and his collaboration with various business leaders within the company enables them to meet their IT and operational objectives.

Tony plays a key role in the technology footprint at the communities managed by FirstService Residential. In this capacity, he provides seamless integration of advanced technology tools, creates efficiencies and establishes reliable connectivity for associates to successfully manage onsite operations and continually provide professional and dependable service.

Tony also helps builders and developers who partner with FirstService Residential to identify and integrate technology needs throughout the construction process to insure a smooth transition to full operation and management.



END-TO-END IT MANAGEMENT

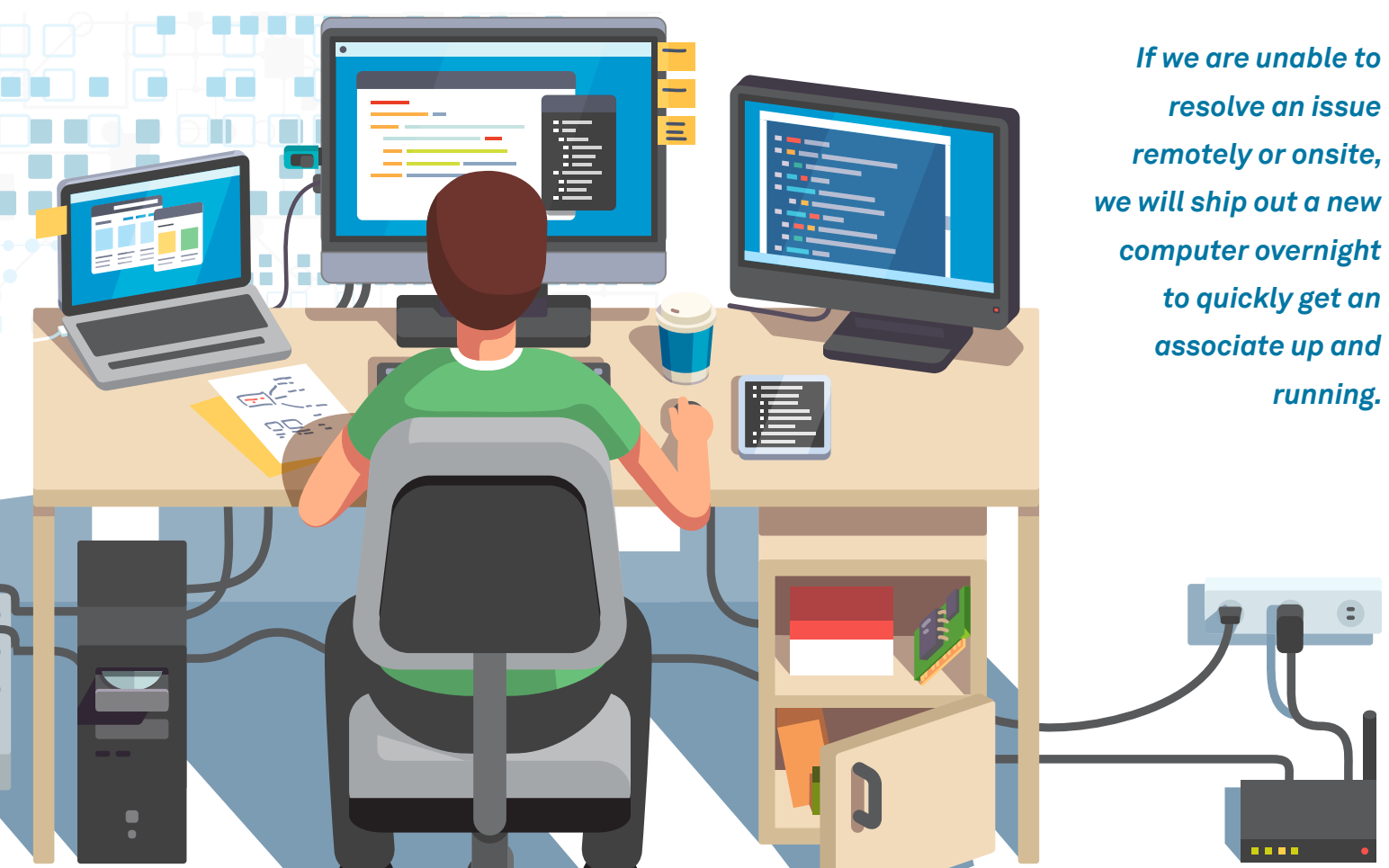
Functioning as part of the FirstService Residential Client Transition Team, dedicated resources evaluate the community's IT infrastructure and determine its specific technology requirements. They then install all of the company-supplied computer workstations and software for onsite associates, based on this evaluation.

The technology we provide to our onsite associates is the same technology that is used throughout FirstService Residential. All equipment and components are owned by FirstService Residential, and we assume full responsibility and liability for them. This means that we handle any repairs or replacements at no additional cost and provide software updates automatically, based on current best practices. All installed software applications are also vetted to be certain that they work seamlessly together.

MINIMAL DOWNTIME

Our goal is to ensure that an association's technology runs smoothly, so we install new, tested equipment at each community. However, equipment issues do happen. To reduce any downtime, our IT staff is available to assist associates remotely or in person with their IT needs. If we are unable to resolve an issue remotely or onsite, we will ship out a new computer overnight to quickly get an associate up and running.

*If we are unable to
resolve an issue
remotely or onsite,
we will ship out a new
computer overnight
to quickly get an
associate up and
running.*





We employ technology with the highest level of security, including robust firewalls and other security measures that protect data systemwide, regardless of where the information resides.

ROBUST SECURITY

Protecting our clients' data is of utmost importance. That's why we employ technology with the highest level of security, including robust firewalls and other security measures that protect data systemwide, regardless of where the information resides. In addition, FirstService Residential uses a range of protections, including authentication, to ensure that access to data is restricted to those users with the appropriate authorization; antivirus and spam filters; malware and intrusion detection; and encryption.

Because we are a large, publicly traded company, FirstService Residential is capable of eliminating potential internal risks by removing local control of data and by separating duties, such as responsibility for payments and receivables. IT audits—including security audits—are conducted regularly to confirm the effectiveness of our security measures. Additionally, we have made substantial investments in technology to enable us to host your data in environments we own and control and to ensure that it isn't jeopardized or shared with other companies.

BACKUPS AND REDUNDANCIES

FirstService Residential conducts a full backup nightly, weekly and monthly. Data is housed offsite at the most advanced data center available on dedicated servers that are monitored 24 hours a day. By housing data at the same data centers that are used by many of the world's leading technology companies—including Microsoft, HP, Intel, Unisys, Intuit and Cisco—we provide our clients with an unmatched level of assurance that their information will always be safe and available, even in the event of a disaster. Backups are also stored offsite at a secondary location to ensure that they are secure, accessible and capable of recreating operations quickly and efficiently if necessary.

When it comes to your data, our goal is to provide your association with peace of mind, not to take control away from you. Your association always retains ownership of your data, and this is spelled out in our contractual agreement with you.

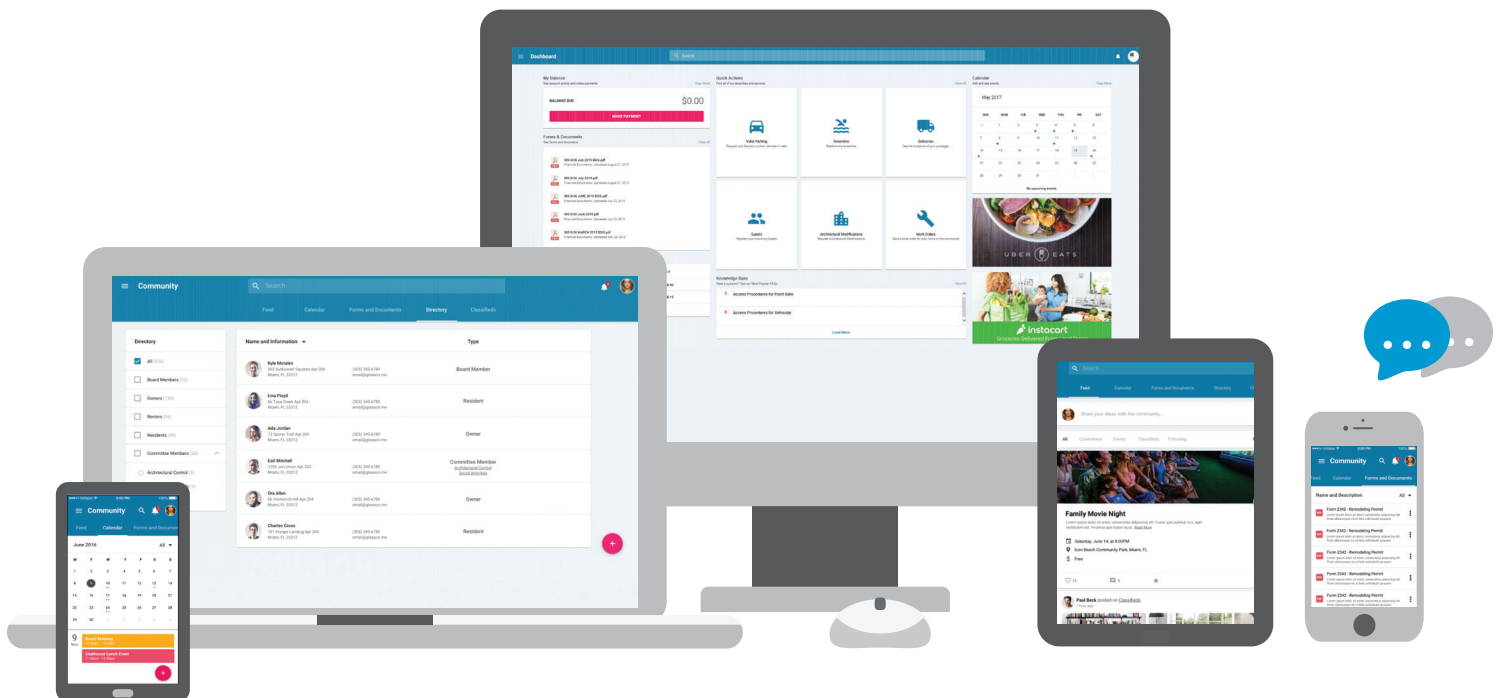
NO UNEXPECTED IT COSTS

Clients pay a flat, per-workstation fee, which is included in the total contracted price for community management services. Repairs, updates, replacements, backups, storage, etc., are provided at no additional cost. This allows associations to easily budget their IT management costs.

POWERFUL HOA MANAGEMENT SOFTWARE

Available exclusively to associations managed by FirstService Residential, our fully owned and integrated management software provides a secure way to connect members of your community. Residents, board members and your management team can communicate and take care of business any time and from any device. The software protects user privacy and limits access based on the user's role within the association.

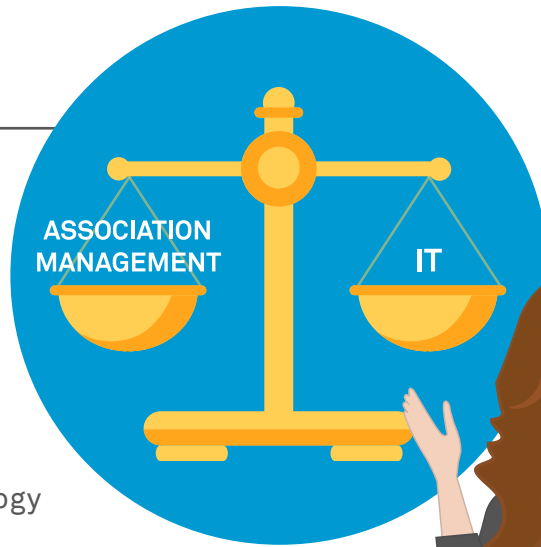
Available exclusively to associations managed by FirstService Residential, our fully owned and integrated management software provides a secure way to connect members of your community.



CONCLUSION

Technology tools can help to significantly streamline your association's day-to-day functions, but they can also make your data more vulnerable. In an era in which small businesses are a prime target for hackers, proper IT management is crucial to protect data and must be a priority for your association. Although there are many technology companies available to help you with this responsibility, there are risks associated with allowing third-party vendors to have access to your information. Furthermore, these companies lack familiarity with the business of running an association.

A good management company will be able to provide you with advanced tools designed specifically for associations and will have the resources, association knowledge and IT expertise to ensure that your data is safe. As you evaluate companies, include an assessment of their IT competencies. Choosing a company that can perform both association and technology management will provide your association with the functionality it needs and the peace of mind it deserves.



Learn more about how FirstService Residential can help you with your IT management. Contact FirstService Residential, California's leading community management company, at learnmore.ca@fsresidential.com or (800) 428-5588.

REFERENCE

- ¹ Symantec, *Internet Security Threat Report*, Volume 21, April 2016.
- ² California Department of Justice, *California Data Breach Report*, February 2016.
- ³ CSID, *Survey: Small Business Security*, May 2016.
- ⁴ CyberScout, *The Evolving Cyber Risks to Small Businesses and Their Data*, September 2016.

About FirstService Residential

FirstService Residential is North America's largest manager of residential communities and the preferred partner of HOAs, community associations and strata corporations in the U.S. and Canada. FirstService Residential's managed communities include low-, mid- and high-rise condominiums and cooperatives; single-family homes; master-planned, lifestyle and active adult communities; and rental and commercial properties.

With an unmatched combination of deep industry experience, local market expertise and personalized attention, FirstService Residential delivers proven solutions and exceptional service that add value, enhance lifestyles and make a difference, every day, for every resident and community it manages. FirstService Residential is a subsidiary of FirstService Corporation, a North American leader in the property services sector.

Over the past three decades, FirstService Residential has grown to become California's premier property management company, serving 950 properties that represent 235,000 units. Twelve regional offices are located in Orange County, North and South Inland Empire, Los Angeles, Westlake Village, Coachella Valley, Santa Clarita, San Diego, Carlsbad, the Bay Area, Sacramento and San Francisco. For more information, visit www.fsresidential.com.



15241 Laguna Canyon Road
Irvine, CA 92618
949.448.6000
www.fsresidential.com
