2022, No. 5

Something Phishy: How to Guard Against Cyberattacks

Cybersecurity should not be the sole concern of your IT Department. Everyone needs to be cyber-aware.

By John Salustri

BOMA International
DEEP DIVE

TABLE OF CONTENTS

THE OVERVIEW

While many of us have either experienced or heard about the immediate and shocking impact of a ransomware attack, hackers and other bad actors can lay seeds of disruption that can remain undetectable for months.

The incidence of such criminal activity and the associated costs seem to be spiraling out of control. According to the FBI's Internet Crime Complaint Center (IC3), in 2021 there were 847,376 complaints, a 7% jump from 2020, and potential losses topped $6.9 billion.

Under the umbrella heading of malware, there are a variety of cyberattack types. As the FBI noted in its report, the most frequent of these last year were ransomware, business e-mail compromise (BEC) schemes and the criminal use of cryptocurrency. BEC schemes alone resulted in 19,954 complaints, with total losses approaching $2.4 billion.

And while attacks can take months to reveal themselves, opening the gates to bad actors can take only seconds. One contributor tells of an email on his personal computer with an attachment that seemed to align vaguely with his work. Two clicks–less than 10 seconds–and all his folders and files, including photos, were renamed with random alphanumeric codes and a digital ransom note. Luckily, many of his files were backed up in the cloud.

To put the issue into a broader context, a recent white paper by JLL predicts that cybercrime will hit $10.5 trillion globally by 2025. Compare this to the U.S. 2021 gross domestic product, which was $20 trillion.

Determining the hit taken by commercial real estate is a bit trickier to gauge. For one, not every operator is a public company, and attacks of this sort do not speak well for public trust and confidence. Negative publicity, then, becomes an ancillary cost of an attack.

"I don't think we really know how big the issue is in commercial real estate, because incidents are largely kept private," one property manager explains. "People sign nondisclosure agreements when they respond to cybersecurity events. But it's obviously a large problem."

For the record, commercial real estate falls under the Commercial Facilities Sector of the 16 critical infrastructure sectors as defined by the Cybersecurity and Infrastructure Security Agency (CISA). This is the arm of the Department of Homeland Security (DHS) leading the national effort to understand, manage and reduce risk to our cyber and physical infrastructure.

We can get a sense of how large a problem it is for commercial real estate by using data provided by the FBI, but the bureau provides only a limited definition: "Loss of funds from a real estate investment or fraud involving rental or timeshare property." This barely covers the breadth of the industry. Nevertheless, these losses in 2021 were $350.3 million–up significantly from the $213.2 million logged the year before.

And that upward trajectory is expected to continue. The term "virus" is an apt term here. As we saw with the recent pandemic, new viral strains attempt to circumvent current remedies. Likewise, cyberattackers, who are diligently working to pierce your latest blocking technology, are making a bulletproof solution virtually impossible.

Moreover, cybersecurity faces an even larger challenge now that more people are working from home, ramping up the exposure risk.

There is little wonder then that the newly released "2023 Emerging Trends in Real Estate", from PwC and the Urban Land Institute, ranks cybersecurity high on the list of technology-driven disruptors, second only to construction technology in order of importance. (Other disruptors–in descending order–include big data, automation, block chain and drones.)

Despite the odds, businesses still need to build in as many protections as possible. But first they need to know, to the greatest extent possible, what they are dealing with.

"There are tons of case studies of the exploitation of OT on buildings that ultimately create nightmares for owners and managers."

–Lucian Niemeyer, Building Cyber Security

CYBERSECURITY 101

We have to begin building our cyber-protections with a sobering fact, warns Wanda Lenkewich, president of the Arlington, Va.-based Chinook Systems: "You have to assume not only that you're going to be breached, but that someone has already hit your network. The ability to detect and negate that breach must be the primary focus."

There are two essential paths to data corruption and loss. The first involves infiltration of your information technology (IT) systems—which can comprise texts, emails and the vacation pictures you share with colleagues. The second is your operational technology (OT) systems. This involves the hardware and software that make your building function, including the lighting, elevator and HVAC controls that can, in the wrong hands, cripple an asset and cause physical harm to people.

"I'd be willing to bet that most people don't even realize that their building automation system is vulnerable," says Tommy Russo, senior vice president of Technology and Engineering Services for Akridge in Washington, DC. He recounts the trouble that this lack of awareness caused for two major retailers.

In 2007, the T.J. Maxx hack was considered the largest ever, with data from 45.7 million credit and debit cards stolen. Six years later, Target Corp. sustained a massive attack that led to an $18.5-million settlement of claims issued by 47 states and the District of Columbia. But the added costs of lost profits (the data breach occurred during the 2013 holiday rush), regulatory fines and legal fees ultimately amounted to $202 million.

T.J. Maxx's Achilles' heel was its operational technology. "HVAC technicians put a new piece of hardware on a rooftop air handler," he says. "It had its own Wi-Fi portal, opening the network to potential exposure, and someone exploited it."

Even more problematic for property managers is the Target hack, which occurred when a trusted HVAC vendor reportedly "fell for a phishing trick and opened an attachment in a fraudulent email the hackers had sent to him."

Remember that these are not mom-and-pop operations, but sophisticated corporate entities. Journalists Woodrow Hartzog and Daniel J. Solove reported in Slate that, "Target had devoted quite a lot of time and resources to its information security. Target had more than 300 information security staff members. The company had maintained a large security operations center in Minneapolis and had a team of security specialists in Bangalore that monitored its computer network 24/7." Just six months before the breach in India, Target had reportedly installed "expensive and sophisticated malware detection software."

Russo carries that sort of intrusion to the next level, one with particular significance in a post-pandemic world: "Say you're running a biotech office and I can turn off the HVAC."

For health and safety as much as data security, "Property managers need to manage the installation of new equipment that will be connected to your building system," he explains. "If your IT department doesn't know about that installation, you've got a problem."

"What would surprise property managers is that, when they do a turnkey buildout for a tenant, for example, inclusive of lighting controls and HVAC systems, the products come unsecured out of the box," Lenkewich says. "That's a huge cybersecurity risk being introduced to your building, and many architectural/engineering firms aren't concerned about it. Nowhere in their design and construction standards is the word 'cybersecurity.'"

One contributor agrees in spirit but does not believe "anything surprises property managers anymore. We deal with such a wide range of challenges every day, and often they're new and different. Maybe what's surprising is how much you could actually do about it ahead of time."

Cybersecurity then can be likened to the modern equivalent of posting a guard at your front and back doors–on the assumption that the guards are trustworthy. As such, it also carries equal significance for your relationships with your vendors.

"Compare it to locks and keys," says one property manager we spoke with. "If everyone had a master key before, and all of a sudden you change all the locks in the building, now everyone has to come to you to check out a key. It changes the way vendors come into the building and perform for you."

Given the state of risk, Lenkewich shared more sobering advice: "We've been operating in a world where we trust but verify. However, we're entering a zero-trust environment, meaning trust no one until they have been verified. Using the door-and-lock analogy, it means not only putting a lock on the main entrance and allowing in a trusted vendor, but also putting a unique lock on every room of the house with user-level authentication and authorization."

"Software needs to be updated constantly because cyberattackers are trying to get at it all the time. The updates you get on your phone are another layer of protection."

–Jason Lund, JLL

RESPONSIBILITY AND RISK

Who then is responsible for keeping bad actors away from the connected, smart technologies of a multi-tenant office building? The short-form answer is: Everyone. But cybersecurity begins not as a team effort but rather as an individual pursuit, with ownership, management, tenancy and vendors watching after their own protections. On the surface, this is a seemingly odd state of affairs in such a service-oriented profession as property management.

"Everyone is essentially on their own," says Jason Lund, JLL's Charlotte, N.C.-based managing director and leader of Technology Infrastructure. "The tenants sign their own technology agreements with different providers, not with the building owners."

But there are nuances here. Yes, on one hand, "There's an understanding that there are unique responsibilities," says Lucian Niemeyer, CEO and board chair of Building Cyber Security, a nonprofit in Bethesda, Md. But that comes with knowing that "a vulnerable tenant can inadvertently initiate and spread an attack through wireless connections to the building management systems and create a risk to the entire building. So those walls have to come down a bit."

"As a property manager in today's society, whether or not the door is locked is the least of your concerns."

–Tommy Russo, Akridge

LOCK IN LEASE LANGUAGE

Niemeyer, a former assistant Secretary of Defense who worked at the Pentagon and the White House, advises that lease language must be carefully worded and properly vetted to avoid legal exposure. “I wouldn’t recommend owners and managers do that casually,” he says, adding that he sees more lease agreements containing “cyber clauses” to delineate responsibilities. “It’s the best way to ensure both parties are clear about roles and requirements to safeguard building and tenant operations from cyber risks.”

Others add that whether you are an owner, manager, tenant or vendor, your IT departments are your first line of defense. But awareness has to spread through the entire stakeholder population. “We’ve taken over lots of buildings in my day,” Russo says, “and a lot of them have four or five different cable or fiber internet service providers.”

The first question is whether these are tenant networks or building networks. “Having that answer, I have to trust that the corporate IT departments have them secured,” he says. “The second question is if I want my building network to be as secure as my tenants’ network.”

That, he says, is where it gets tricky, because “property managers are not technologists. But they have to ask those questions.” The IT department can build in the safeguards. But “it’s in the property manager’s bailiwick to communicate between tenants and IT departments.” And asking the right questions requires a level of knowledge and training that then provides for the ability to identify and mitigate risk.

Where does the building engineer fit in this scenario? Cybersecurity is not their forte, Russo states. While they will focus on building systems, “they’re thinking in terms of motors, pumps and fans, not switches, routers and IP addresses.”

When it comes to a building’s exposure to risk, that is an issue that falls to building ownership. The owner must first understand the risk to human safety and property posed by the technologies in a building, and then determine the best approach to manage the risk.

As Niemeyer points out, “Insurance is the byproduct of risk. Property owners will assume cyber risk, mitigate it through investments or transfer it. The insurance industry is in the risk-transfer business, and they have their own interests in mind to minimize their own liability and exposure.”

That is evident in the direction of rates and the proliferation of policy carve-outs. Niemeyer recalls a time when attacks were relatively scarce and cyber policies came with reflectively low rates. Now, with the explosion of claims, “rates are rising—as much as 300%—while exclusion clauses widen. You may not be able to execute a claim because of the fine print.”

As Lund states in the JLL white paper, "Building owners should know the requirements of their accountability for transparency regarding cybersecurity incidents. This is the type of information we want our clients to know is potentially on the horizon, so they can be prepared for it."

Armed with that information, owners should pore over existing policies to understand, "precisely what level of cyber coverage, if any, is included in response to the wide range of potential cyberattacks. This process will help uncover areas where potential gaps exist."

Without such safeguards, Niemeyer says, "We believe it will be increasingly untenable to continue to transfer risk, so you've got to take steps to reduce it."

RISK REDUCTION–STEP-BY-STEP

Cybersecurity is, of course, a national issue, and the Department of Homeland Security is on the case. Among the programs fostered by DHS are the Joint Cyber Defense Collaborative, Shields Up, the creation of the Cyber Safety Review Board, and the announcement of $1 billion in cybersecurity grants for state and local partners. (*It also declared this past October Cybersecurity Awareness Month. See "DHS's Four-Point Cyber Plan," page 13.*)

"The grants are a good start," says Niemeyer. "But I'm concerned about how to implement them in such a way that they'll truly have a tangible impact. Homeland Security wants to target water systems and public infrastructure, but there are 55,000 water systems across the country."

Lenkewich agrees, both on the good intentions (supply chain protections and cyber-workforce development are both part of the DHS outline) and the problem of doling out the funds. "Five million dollars allocated to each state won't go very far," she says.

This is just one of the reasons our speakers advise property professionals not to leave their security up to the government. You are better served at the hands of your IT department, that first line of cyber-defense. But there are checks and balances throughout the organization, and a constant awareness of potential breaches that must be maintained. There are practical steps you can take now to secure your digital perimeters.

Here is what Lund says are the types of controls insurance companies typically want to see:

- **Multi-factor authentication (MFA).** All team members must verify their identity as they log in. At this point, we have all gone to our backup devices to find an automatically generated code as that verification. MFA is also a key principle of the DHS program.

- **Password control.** Linked to MFA is the need to change passwords "on a regular basis," says Lund, who adds that companies also tend to get "sloppy about turning off user IDs and passwords once an employee leaves."

- **Endpoint detection and response.** Simply put, explains Lund, "Any place where a wire terminates at a device is an endpoint." Whether we're discussing Wi-Fi or wired systems, "You can see what's touching each of them with a good quality network operations center."

  Here, by the way, we might ask, how safe is the cloud. Not surprisingly, as Lenkewich indicates, "The adversaries are also focusing on hitting the weak points in cloud implementation. Secure encrypted communications are critical, as are secure configurations of the application programming interface (API) connecting various applications together."

  The major vulnerabilities lie in those endpoints in your building. "The cloud itself–the collection of data centers around the world–is pretty darn safe," says Lund. "Access in and out of it is pretty darn safe as well."

- **Patch management.** "In your stack of equipment there are electronic boxes that run the software that manages all this stuff," he says. "That software needs to be updated constantly because cyber attackers are trying to get at it all the time." Patching is simply doing the recommended updates, but you need to do them. "It's a big problem because a lot of people don't update their software."

- **Secure remote access.** Here is where the recent explosion of work-from-home protocols sent security concerns into overdrive. "Those endpoints have to be secured and monitored as well."

- **Disaster recovery plans.** Not to be confused with redundant backup. "Resilience is the big thing," says Lund. "It's all about speed, how fast you catch something, how fast you can isolate and stop it and how fast you can assess and repair the damage."

- **Backups and email filtering.** As we have seen, emails are a favorite access point for hackers. So filtering is key. "Good companies will also have regular programs where they will phish their own employees with mock attacks." These, he says, are the digital equivalent of fire drills.

- **Properly architected user-management and service accounts.** "You need to manage security to the same level of protections up and down the entire reporting structure," says Lund.

- **Cyber awareness.** As stated, cybersecurity is everyone's concern. This is where the above-mentioned knowledge and training come in. Property managers may not need to know how to configure a line of defense. They do need to know exactly how vulnerable they may be.

Toward that end, much is being done, says Lund, particularly at the level of the larger institutional players. "There's more vulnerability in smaller management firms," he says. "But there's also less automation, so there's a sort of balance."

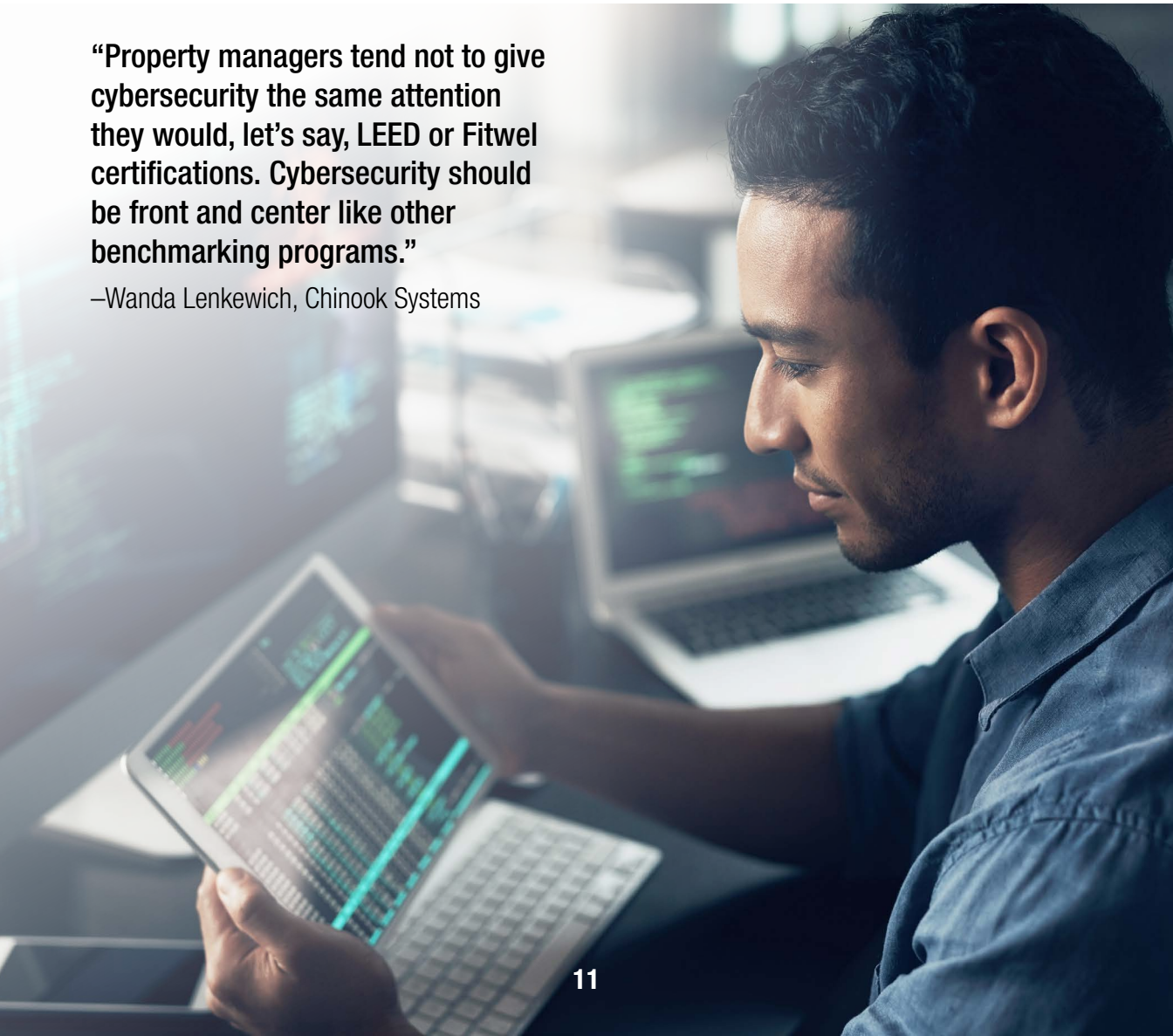
Company size aside, full cybersecurity is in part a cultural consideration, especially given the zero-trust environment we have entered. "You're developing a new relationship with your vendors that you never had before," says one contributor. "It's a big cultural shift. The practicalities of how you work with all of your vendors is changing."

Lund agrees, especially if a new technician appears at your door. "If you're a property manager, you need to figure out who they are and who they're with. You need to see their work order and their license. Then call that firm and verify why they're here." If we learned anything from the T. J. Maxx and Target hacks, it is that "physical access onto rooftops and into equipment closets can create problems." It should be noted here, of course, that not all breaches stem from malicious intent. The cause can also be basic carelessness.

Russo calls this new culture a changing paradigm and explains that he has a third-party provider come in once or twice a year to do a penetration test, an assessment of in-house vulnerability. As an extra layer of protection, he switches providers from test to test.

"It's never the same vendor," he says. "I want them to start from scratch, rather than simply testing for any vulnerabilities they may have found previously. I give them every bit of information they ask for and then I say, 'Come get me.'" But penetration tests do not run cheap, he adds, starting at about $7,000 for a multi-asset portfolio.

Which, of course, brings up the issue of cost/benefits.



"Property managers tend not to give cybersecurity the same attention they would, let's say, LEED or Fitwel certifications. Cybersecurity should be front and center like other benchmarking programs."

–Wanda Lenkewich, Chinook Systems

WHAT PRICE PROTECTION?

Cost considerations need to be balanced against what it is you are protecting. At the very least, there is the access to and the integrity and reliability of your data. At worst, there is the health and safety of your building population, especially when utility, HVAC and elevator controls can fall into the hands of bad actors.

"Cybersecurity is now a matter of cybersafety," says Niemeyer. "Are our tenants safe? Is there some vulnerability we need to address to reduce the risk of an unsafe condition?"

Of course, there is what Lenkewich refers to as the low-hanging fruit, such as sharper password protocols. But then you have to remember the aggressive nature of your unseen adversaries. "Once those things get locked down, the bad actors begin looking for the next vulnerability."

As with most products and services, "Costs can get as expensive as you want," says Lund. "But when you compare the cost of prevention versus the cost of loss, the loss is always much worse. Reputational damage is very hard to quantify, but it's damaging nonetheless."

Ditto the cost of lawsuits.

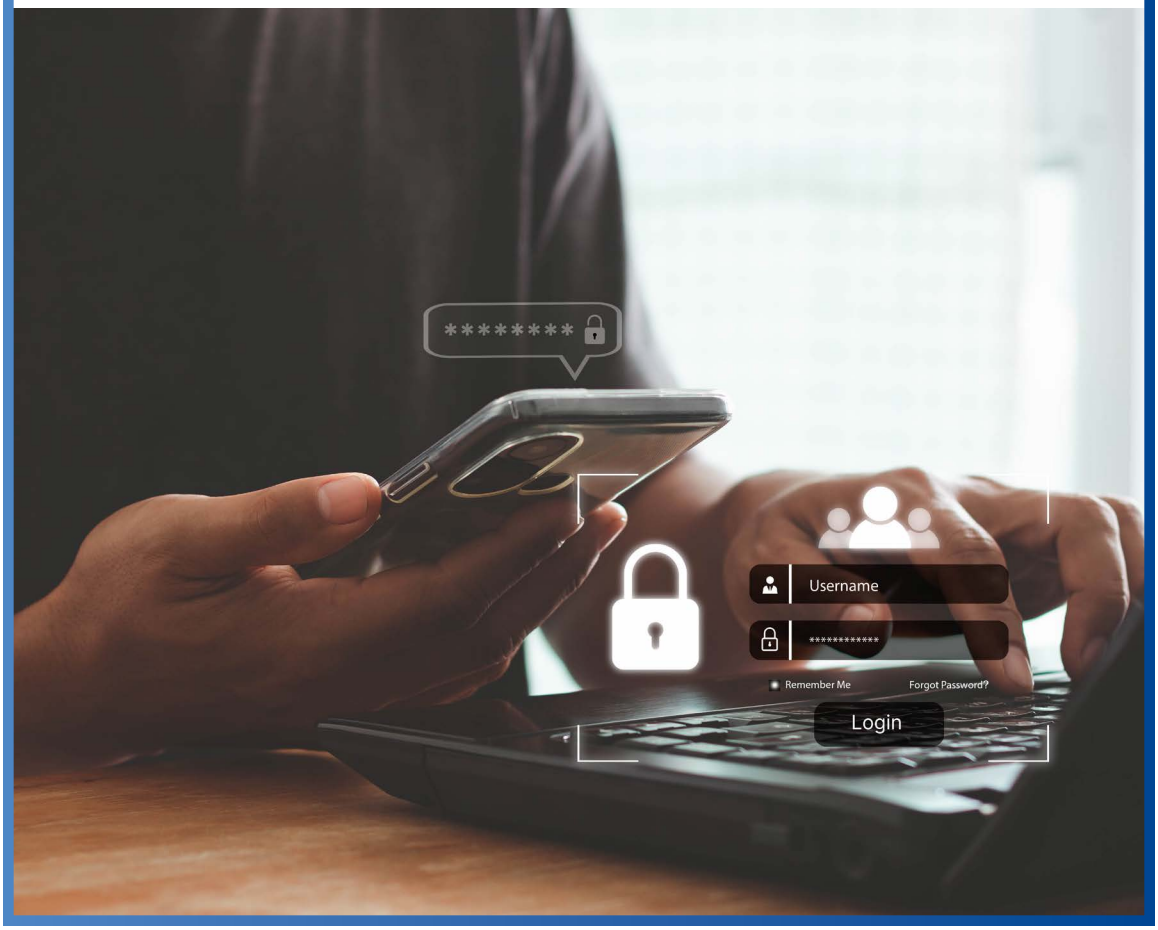
Therein lies the irony of creating a safe and secure environment. On one hand, little of this was even a topic of conversation a few years ago. Still, an age-old refrain applies:

An ounce of prevention …

DHS's Four-Point Cyber Plan

Administered through the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Homeland Security's Cybersecurity Awareness Month this past October focused on education and direction to strengthen an organization's digital safeguards. The wisdom found within, of course, is applicable throughout the year. Here is this year's four-point plan:

- **"Think before you click:** Recognize and report phishing: If a link looks a little off, it could be an attempt to get sensitive information or install malware.
- **"Update your software:** Don't delay. If you see a software update notification, act promptly. Better yet, turn on automatic updates.
- **"Use strong passwords:** Use passwords that are long, unique and randomly generated. Use password managers to generate and remember different, complex passwords for each of your accounts. A passwords manager will encrypt passwords, securing them for you.
- **"Enable multi-factor authentication:** You need more than a password to protect your online accounts, and enabling MFA makes you significantly less likely to get hacked."



ACKNOWLEDGMENTS

Generously sharing their time and expertise were:

Wanda Lenkewich, President, Chinook Systems, Arlington, Virginia

Jason Lund, Managing Director, Leader of Technology Infrastructure, JLL, Charlotte, N.C.

Lucian Niemeyer, Chief Executive Officer, Building Cyber Security, Bethesda, Maryland

Tommy Russo, Senior Vice President of Technology and Engineering Services, Akridge, Washington, D.C.

(Note: Due to the nature of the subject, certain property managers interviewed for this Deep Dive chose to keep their names and companies anonymous.)

Research work contributing to this paper includes:

From Cybersecurity and Infrastructure Security Agency:
"Cybersecurity Awareness Month."
https://www.cisa.gov/cybersecurity-awareness-month

From the Federal Bureau of Investigation:
"Internet Crime Report, 2021."
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

From JLL:
"You May Not Have the Cyber Insurance Coverage You Think You Do," October 2022.
https://drive.google.com/drive/u/0/folders/1F-C2EJDXH5JU5fXcN3qUXcodRNyE9rS5-

From NBC News:
"T.J. Maxx Theft Believed Largest Hack Ever," by Mark Jewell, March 30, 2007.
https://www.nbcnews.com/id/wbna17871485

"Target Settles 2013 Hacked Customer Data Breach for $18.5 Million," by Reuters, May 24, 2017.
https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031

From PwC and the Urban Land Institute:
"2023 Emerging Trends in Real Estate."
https://www.pwc.com/us/en/industries/financial-services/asset-wealth-management/real-estate/emerging-trends-in-real-estate.html

From Slate:
"We Still Haven't Learned the Major Lesson of the 2013 Target Hack," by Woodrow Hartzog and Daniel J. Solove, April 13, 2022.
https://slate.com/technology/2022/04/breached-excerpt-hartzog-solove-target.html#:~:text=Through%20the%20Trojan%20horse%2C%20the,just%20a%20few%20thousand%20dollars.

Photography Accreditation
Cover: KanawatTH / iStock / Getty Images Plus
Page 3: jeffbergen / E+ / Getty Images
Page 5: anyaberkut / iStock / Getty Images Plus
Page 6: gorodenkoff / iStock / Getty Images Plus
Page 8: metamorworks / iStock / Getty Images Plus
Page 11: PeopleImages / iStock / Getty Images Plus
Page 12: guvendemir / iStock / Getty Images Plus
Page 13: tsingha25 / iStock / Getty Images Plus