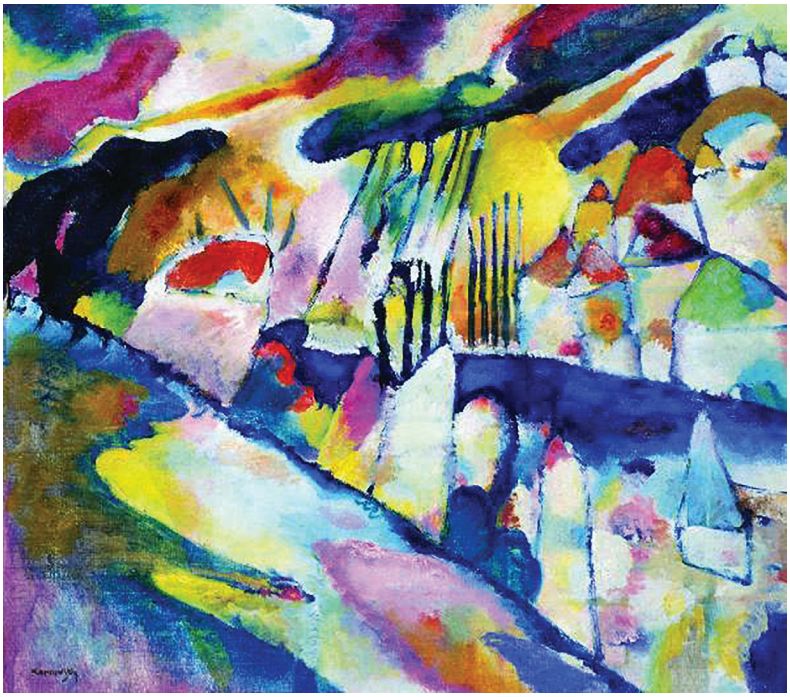
# Institutional Real Estate
*Americas*

The investor-focused global real estate publication



# How solid is your cybersecurity plan?

*More technology means more avenues for intrusion*

by Lauren Stokes

In today's world of digital transformation — with data proliferating, transactions moving online and the Internet of Things connecting everyone with everything, cybercrime is one of the biggest threats facing nearly all organizations. Those engaged in commercial real estate are no exception, yet many are alarmingly unprepared.

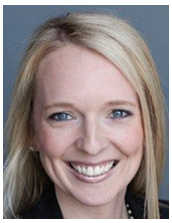
Although, to date, the commercial real estate industry has not been a primary target for cyberattacks, it is not immune. In September 2014, a publicly traded REIT that specializes in West Coast multifamily residential properties reported a cyber intrusion on its computer networks that contained personal and proprietary information. The breach actually occurred before April of that year, with evidence some systems had been compromised as far back as August 2013 — almost a year before the problem was reported.

The fallout was significant.

In fourth quarter 2014, the REIT recorded $2.8 million in attack-related expenses, including costs for legal and investigative fees, communications with the company's lessees and employees, and the provisioning of identity protection services. The business also got hit with a class-action lawsuit alleging it failed to properly secure residents' personally identifiable information. And then, no doubt, was the incalculable cost to the REIT's brand, both at the time and in the following years.

In recent years, we have been witnessing dramatic rises in cybercrimes across a broad range of real estate sectors. The cybercriminals' toolkits and methods have continuously become more sophisticated, and increasingly include the use of automated cyberbots to broadly infiltrate networks and systems with even greater stealth. Although actual dollar figures are not yet available for 2018, Gartner, a leading technology research and advisory firm, predicted global spending on information security products and services in 2018 would exceed $114 billion, an increase of 12.4 percent over 2017. Gartner forecasts the market will grow 8.7 percent to $124 billion in 2019. And the pace of market growth appears to be accelerating exponentially. By 2021, cybercrime damages are expected to cost businesses worldwide more than $6 trillion annually, according to Cybersecurity Ventures, a publisher of information about the global cyber economy. Per the publisher, this includes but is not limited to "the cost of damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm."

***It is no longer a question of "if" your business will be victimized; it's now simply a matter of "when."***



**Lauren Stokes**
**RealFoundations**

It is no longer a question of "if" your business will be victimized; it's now simply a matter of "when." Nevertheless, many commercial real estate companies are not adequately protecting

themselves from potential attacks, nor are they set up for timely detection, containment and mitigation. In the event of an incident, they almost certainly will suffer highly disruptive and costly impacts, as well as reputational damage.

Phishing is one of the most common types of cyberattacks. Although phishing can take a number of forms, the perpetrators' goal almost always is to get victims to share sensitive information, such as login credentials, credit card information and/or bank account details, which they then use to steal funds. Following are examples:

- **Phishing:** Hackers impersonate a real company to obtain your log-in credentials. You may receive an email asking you to verify your account details. The note includes a link that takes you to an imposter log-in screen, which delivers your information to attackers.
- **Spear phishing:** The criminal sends you an email with customized information, such as your name and phone number. This tricks you into thinking the sender has a connection to you and is legitimate, so you will click on a link or attachment, and then share private details.
- **Whaling:** This is a ploy for getting you to transfer money or to email sensitive information, such as usernames and passwords, to an attacker who is impersonating a company employee. Using a fake domain that resembles the company domain, whaling emails mirror corporate emails and often appear to come from senior executives at your business.
- **Shared document phishing:** You might receive an email that looks like it's from a file-sharing site, such as Dropbox or Google Drive, with an alert the sender or another party has shared a document with you. A link in the email takes you to a fake log-in page that mimics a real one and ultimately captures your account credentials.

Clearly, cybersecurity must be an organizational priority starting in the C-suite. It is not strictly an IT problem. The executive team must make it a focus for the entire enterprise by developing a comprehensive strategy and implementing a rigorous tactical plan. Supporting these efforts with a sufficient budget is critical. The following key activities should be included in your cybersecurity plan.

**Secure the technology perimeter** by hardening networks/infrastructure through the following key practices:

- Multifactor authentication, which requires a user to enter at least two forms of evidence, (e.g., a valid username/password combination, answers to personal questions) to log in to an account.
- Location-based policies or geofencing, which restrict access to information or systems (e.g., email) from locations outside of predefined boundaries.
- Use of antivirus/antimalware to guard against online viruses and malware threats.
- Ongoing vulnerability assessments to identify weaknesses in the organization's technology environment and establish mitigation procedures.
- Penetration testing, which simulates the activities a hacker might use to exploit and gain access to information and systems.
- Ongoing patch management so software patches are applied timely to fix security vulnerabilities and other bugs.
- A strong intrusion detection and prevention program that uses tools and programs to monitor events inside a network, and quickly identify and thwart potential violations.
- Elevated audit and logging, which provide more detailed information about activities occurring in your organization's technology environment, such as the time, source and nature of unauthorized access and/or changes.

**Institute leading practices, policies, procedures and governance,** including enforceable policies and plans. These should cover: password strength, technology security, mobile devices, incident response and content retention.

**Educate employees** so they recognize, report and don't fall victim to suspicious activity. Regularly conduct cybersecurity training and phishing tests.

Safeguarding your business from cybercrime is a demanding, ongoing function. Technology is continuously changing, as are the tactics these thieves employ. Keeping up with the steady stream of new information and evolving best practices is very challenging. Whether a company handles cybersecurity on its own or via outsourcing, the most important thing is to have a dedicated, well-funded, organization-wide program in place. ❖

**Lauren Stokes** is a director with **RealFoundations,** based in Dallas.