KPMG

Securing real estate assets in a digital world

How internal audit can focus your organization's cybersecurity

kpmg.com

Real talk about real estate cybercrime

We've all heard the warnings: Cyber-attacks continue to escalate, and it is truer than ever that every company in every industry is at risk.

In 2016 alone, hackers compromised 500 million accounts from a major email provider, leaked 19,000 emails from U.S. political party officials, stole $81 million from a foreign bank, and even brought down major parts of the Internet[1].

Infosec Institute predicts that, in 2017, "the number of cyber-attacks will continue to grow in almost every industry[2] and BI Intelligence estimates "$655 billion will be spent on cybersecurity initiatives to protect PCs, mobile devices and Internet of Things (IoT) devices between 2015 and 2020[3]."

With high-profile breaches making headlines on a regular basis, CEOs across industries named cybersecurity as the biggest risk facing their businesses, according to KPMG's 2016 CEO Survey[4].

But is cyber risk a real problem in commercial real estate? What specific cyber threats are most likely to affect real estate firms? And what steps can real estate leaders take to proactively prepare their organizations to protect valuable data and assets from cyber attackers?

This paper explores these questions and provides practical insights real estate leaders can take to get started protecting their companies from cybercrime. Like many other risks to a real estate firm, KPMG's view is that internal audit can drive an objective focus on your firm's specific cyber exposure and response capabilities.

[1] Here's how cyber-attacks get worse in 2017 (Venture Beat, December 11, 2016)
[2] 2017 Cyber Security Predictions (Infosec Institute, Dec. 19, 2016)
[3] This one chart explains why cybersecurity is so important (BI Intelligence, April 5, 2016)
[4] U.S. CEO Outlook Survey (KPMG, 2016)

Highlights

— The value of a real estate company's intellectual property may be rapidly approaching the value of its physical assets.

— Data breaches are a real and imminent threat in the real estate sector, with potentially catastrophic financial, reputational and legal consequences.

— Real estate leaders must heed the call to ramp up capabilities to secure real estate assets from cybercriminals. But many don't know where to start.

— The internal audit capability plays a critical role in the battle against cybercrime—providing executives an initial roadmap of the real threats or providing ongoing assessments of emerging cyber risks and current cybersecurity strengths and weaknesses that inform smart decisions to strengthen defenses.

Yes, it can happen to you

Real estate is an industry of real, tangible assets—from office buildings and shopping centers, to hotels and entertainment properties, to houses and apartments, to factories and farmland. So it's no wonder that historically real estate executives have mostly been concerned about the physical security of their properties from theft, damage, and natural disaster. Protecting invisible bits of information somewhere on a network from falling into the wrong hands probably just didn't seem so urgent, especially since the household-name corporations that have suffered newsworthy cyber-attacks are primarily concentrated in the retail and financial services sectors. These targets often have millions of transactions and records in play—many more than the typical real estate company.

But today, data, connectivity and digitization are playing an ever-increasing role in every business—commercial real estate included. As a result, the attack vector has increased significantly.

As real estate businesses become more reliant on technology, their decision-makers are realizing that they are not immune to cyber threats and that data breaches in this industry are real. In fact, the real estate industry should now be considered a vulnerable and high-value target. Cyber-attackers have specifically targeted real estate companies in a string of breaches in the past few years.

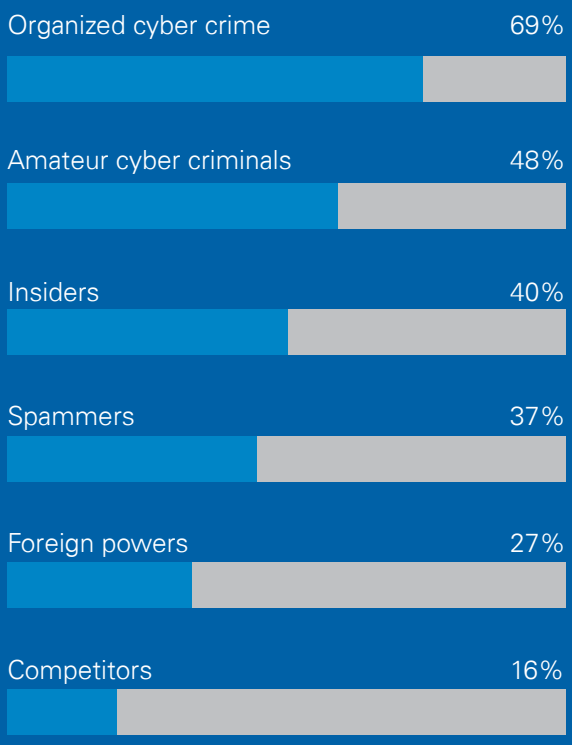
Consider some of the specific vulnerabilities that make real estate companies attractive targets to hackers.

- Real estate company technology systems contain leases, rental applications, credit reports, and deal financing terms—all filled with payment card industry (PCI) data and personally identifiable information (PII) on tenants and clients.
- Real estate professionals regularly pass confidential data back and forth through email, mobile devices, and cloud-based business applications.
- Apartment, retail and office assets are wired and computerized, creating potential intrusion vulnerabilities through connected technologies like smart alarms, locks and lights, environmental controls and voice-assisted devices.
- Real estate investment trusts (REITs) manage huge sums of money online and could even be targeted for the cash from transactions handled by their internal systems.
- Real estate owners and operators of properties with high-profile tenants may be targets of cyber-attacks intended to ultimately steal secrets or financial information from those tenants.
- All service providers to the organization, or those operating in or around a real estate company's properties, may end up posing a cyber risk, as a vulnerability in a service provider's cybersecurity could expose the extended network.

Who's out to hack you?

Chief Information Officers (CIOs) are most concerned with the risk of cyber-attack by organized criminals, followed by amateur cyber criminals. Only four in 10 think insiders—current or former employees—present a comparable cyber risk.

Which types of threat give you most cause for concern in terms of a cyber attack?



[5] The Creative CIO: Harvey Nash/KPMG CIO Survey 2016 (Harvey Nash/KPMG, 2016)
data is global and cross-industry

Cost of cybercrime

The probability an organization will experience a material data breach is 26% in the next two years.

— A material data breach involves 10,000+ lost or stolen records.

— Malicious or criminal attack is the most common root cause of a data breach (48%), followed by system glitch (27%) and human error (25%).

The cost incurred for each lost or stolen record is $158.

— The average size of a data breach—the number of records lost or stolen—is 23,834 records, an increase of 3.2% since the 2015 study.

— The cost of a lost or stolen record increased 2.9% since the 2015 study.

The average total cost of a data breach is $4 million.

— The cost includes direct and indirect expenses incurred by the organization. Direct expenses include engaging forensic experts to aid in the organization's investigation, outsourcing hotline support to communicate with impacted stakeholders, and providing free credit monitoring subscriptions and discounts to impacted stakeholders. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

— The average cost of a data breach increased 5.4% since the 2015 study.

[6] 2016 Ponemon Institute Cost of a Data Breach Study sponsored by IBM' (Ponemon Institute, June 15, 2016)
data is global and cross-industry

Real cyber-attacks in the real estate sector

— A management company operating hotels for some of the industry's most recognized brands discovered malware in payment systems at 20 properties, likely affecting tens of thousands of customers[7]

— A thief infiltrated a large database of commercial properties and stole $360K in records from a real estate information provider[8]

— An infamous cyber-attack in which hackers stole personal information from tens of millions of customers of a major retailer was sourced back to the retailer's HVAC contractor[9]

[7] Starwood, Marriott, Hyatt, IHG hit by malware: HEI (Reuters, Aug. 14, 2016)
[8] Data pirate stole $360K in real-estate records: lawsuit (New York Post, Aug. 30, 2015)
[9] Target breach happened because of a basic network segmentation error (Computerworld, February 6, 2014)

KPMG

"Cybersecurity is not simply a technical issue, and securing your IT systems is only part of the story. You must also protect against the human element. That includes the 'insider threat'—cybercriminals working for your organization or connected third parties—as well as competitors or nation-states that might steal your intellectual property by compromising staff or breaking in. Are your security systems modern and tested? Have you vetted your suppliers and contractors? Is cybersecurity part of your third-party contracts and policies? Is security a holistic initiative in your firm, with employees acting as your 'agents?' Does your culture prioritize security? These are all security areas that real estate companies may be overlooking."

Ian McPherson,
KPMG Advisory Principal, Justice and Security practice

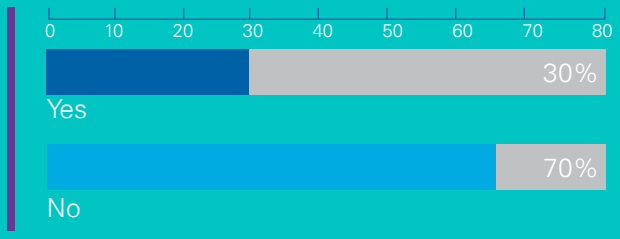
Ready or not ...

KPMG's 2017 Real Estate Industry Outlook Survey reveals that real estate leaders largely recognize their company's increased cyber risk exposure in the digital age. Close to one-third of real estate leaders (30 percent) surveyed reported that their company had experienced a cybersecurity event in the previous 24 months[10].

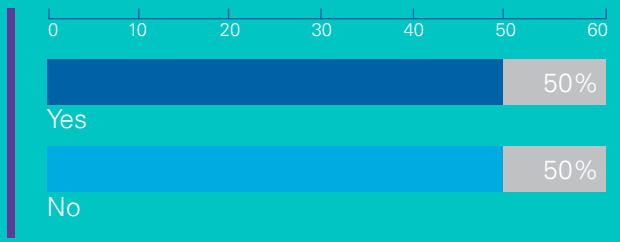
The survey's findings are broadly consistent with cross-industry research on the cyber threat. A Harvey Nash/KPMG survey of global Chief Information Officers (CIOs) found that more than a quarter of companies across 19 industries—28 percent—had to respond to a cyber-attack in the same span of time[11].

Despite the clear-and-ever-present danger cybercrime poses, many real estate companies say they are ill-prepared to prevent or mitigate an actual cyber-attack. Only 50% of respondents to KPMG's 2017 Real Estate Industry Outlook Survey said they are adequately prepared to prevent or mitigate such an event[12].

Has your firm (or one or more of your properties) experienced a cybersecurity event within the last 24 months?



Do you feel you are adequately prepared to prevent or mitigate a cyber attack?



[10] KPMG Real Estate Industry Outlook Survey (KPMG, 2017)
[11] The Creative CIO: Harvey Nash/KPMG CIO Survey 2016 (Harvey Nash/KPMG, 2016)
*data is global and cross-industry
[12] Real Estate Industry Outlook Survey (KPMG, 2017)

Where Internal Audit can make a difference

The first step is admitting you have a problem—and today's heightened cyber threat leaves no doubt. Most real estate leaders are now convinced that a data breach is probably not a question of "if?" but "when?" As such, many realize the importance of developing or enhancing cybersecurity within the organization.

The internal audit function should play a critical role in contributing to a sound cybersecurity program. If a real estate organization lacks a cybersecurity program, internal audit can provide an objective initial assessment to guide the development of a program right-sized to the organization's level of risk exposure. Once a cybersecurity program is in place, internal audit can provide strong oversight—an imperative given the always-evolving threat landscape and the vast complexity of cybersecurity protection from an organizational and technological standpoint. After all, appropriate protection today may be obsolete tomorrow.

The foundation of a strong cybersecurity program should be assessments of cyber risk, readiness and capabilities, conducted by internal audit. Internal audit cyber reviews typically focus on evaluating existing and emerging cyber risks, assessing the ongoing state of security within the organization, and gauging how companies compare to peers and industry standards when it comes to cybersecurity.

Internal audit assessments help real estate CEOs and boards understand the organization's security strengths and weaknesses so they can design and implement an effective strategy to protect their organizations from cybercrime. Working in close collaboration with operations and IT, internal audit assessments give leaders the information they need to prioritize where to focus security initiatives by identifying the weakest and most vulnerable areas of the security environment.

Where to focus your cybersecurity efforts

There are a number of key areas where internal audit should particularly focus their cyber reviews.

Perimeter protection: As real estate companies become more high-tech, mobile and connected, the universe of people with access to their systems and data expands. Any one of these people or organizations could pose a threat, whether they are a well-intentioned staffer who doesn't understand how to securely handle data, a disgruntled employee harboring a grudge, or a third-party vendor with insufficient security programs. In this new landscape, internal audit can ramp up assessments of cyber awareness training, identity and authentication, security intelligence methods, and protocols for accessing, storing, sharing and securing information.

Critical data protection: If a cybercriminal is a thief, data is the shiniest jewel. In the real estate industry, that critical data includes corporate intellectual property as well as investor listings and holdings containing PII and sensitive financial information. Internal audit reviews can provide careful oversight of privacy policies and other safeguards related to classifying, storing and accessing the most valuable data an organization currently manages.

Incident response: All real estate companies should have a formal cybersecurity incident response plan in place, so, when an incident does occur, they can minimize the damage. The plan lays out action steps from both a business and a technical perspective, defining what individual people and teams do to stop the intrusion from spreading, re-secure the network, investigate the incident, communicate with customers, and more. Internal audit reviews can ensure the plan works and that it is regularly tested and updated as threats evolve, including addressing relevant incidents that occur outside of their organization.

Reporting to top leadership: Cybersecurity should be viewed as more than a technology risk. It's a business risk, too. Internal audit can assess whether senior executives outside of IT, even all the way up to the audit committee, CEO and the board, have clearly defined roles and responsibilities for designing, implementing and overseeing policies and processes for mitigating cyber risk—and that each person meets his or her critical responsibilities.

Reporting to stakeholders: External communication is often where organizations fall short in managing cybersecurity incidents. Internal audit can validate the ability of the organization to communicate relevant, appropriate and timely information about a cybersecurity event to all affected outsiders, such as shareholders, investors, customers, the board, the press, or members of a family office. For example, does the organization have a standardized template for public relations and marketing communications to inform stakeholders that an event occurred, what the organization knows and doesn't know, how the organization is investigating, and where people can go to get more information?

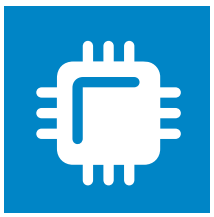
Below are four types of audits that can deliver this vital knowledge, enabling real estate leaders to design a stronger cybersecurity defense, accelerate key implementation action steps, get ahead of exposure, and quickly course-correct as new challenges arise.

Cyber maturity assessment

In the past, security assessments have often focused on a particular technology or technical area, whereas robust security assessments should include a holistic assessment of a security program. KPMG defines the primary dimensions of security (referenced in the graphic) and always develops a rounded view into the people, process and technology supporting the program. The objective of any effective cyber maturity assessment is to identify gaps in the present cyber security posture, understand the scope and scale of any vulnerabilities and prioritize the required remediation activities. A top-down evaluation of the overall maturity of the cyber function that looks beyond pure technical preparedness against cyber-attack is a particularly powerful audit area. It provides senior management with a holistic view of security risk to the organization. And, in no uncertain terms, it reveals how well the security program can meet that risk. This knowledge enables the organization to prioritize where to allocate resources to mitigate the highest areas of risk.

Thematic audits

Thematic audits are comprehensive end-to-end assessments of key processes and controls across the business. For example, internal audit might evaluate the cyber risks posed by a specific type of enterprise technology, such as a rent payment system. Or they might look at the effectiveness of security controls around an organization's highest priority data, such as vulnerabilities in the protection of sensitive data of a particularly high-profile tenant. Or they might review the cybersecurity-related contractual responsibilities of tenants, operators or joint venture partners.



New technology audits

Emerging technology platforms such as cloud, mobile, social, big data, IoT devices and robotics introduce new cyber risks, and therefore warrant their own audits. This audit type includes application-level security assessments as well as pre- and post-implementation reviews of security environment related to new technologies.

Deep technology audits
Particularly sophisticated technology, such as ERP systems, database management systems and payment systems, also create cyber vulnerabilities. KPMG is seeing increasing levels of investment in larger-scale technology systems in the real estate industry. What's more, the often patchwork nature of these systems due to a lack of a holistic technology architecture serves to increase risk exposure. As such, it is important for internal audit to assess the specific security risks related to these critical technologies and the information they contain. It is also important that the reviews span across the application, operating system and platform level in order to gain a comprehensive understanding of security risks.

Primary dimensions of security

Final thoughts

Real estate companies and individual properties are prime, high-value targets for cybercriminals seeking to steal confidential corporate information, money, credit card information, private account data, and consumer identities. The risks go far beyond data loss: The financial, regulatory and reputational impact of a cyber-attack can be even more damaging to the long-term success of your company's brand, including your relationships with all of your critical stakeholders.

As protecting assets of all stripes has become a key concern within real estate, internal audit has the opportunity to play an active, central and vital role.

After all, you can't fix a problem if you don't understand it. By providing an initial view of the organization's cyber exposure and a roadmap to address it, as well as conducting periodic reviews of both cybersecurity exposures and response plans, internal audit is an integral player in helping real estate executives achieve better cybersecurity and protect their organizations from this very real threat.

About the authors

Michael Smith is a partner in KPMG Advisory, working with companies in the real estate, asset management and power and utilities sectors. Michael has almost 20 years of experience leading risk and control programs, including process and controls assessments, internal audits, enterprise risk assessments, and SOX programs. His approach enables clients to focus on process and control improvements while balancing effective risk management and cost efficiency objectives.

Sean Gleason is a director in KPMG's Advisory practice. He has more than 15 years of financial services experience in asset management and capital markets with a heavy focus on driving value for asset managers through use of internal audits and internal control assessments. Most recently, he was the global head of IT audit, risk and control for a large multinational private equity firm which included real-estate-specific platforms. He also worked in various leadership roles assessing process and control risk for a top-tier international investment bank.

Andres Cools is a leader in the cybersecurity practice with KPMG Advisory, specializing in cybersecurity strategy and program assessments, threat and vulnerability assessments, vulnerability and information risk management, and build-out of cybersecurity operations centers. He has more than 18 years of experience in information security leadership roles, performing delivery, delivery management, and business development.

About KPMG's real estate practice

KPMG LLP advises owners, managers, developers, lenders, intermediaries, construction and engineering firms, and investors in effectively executing complex transactions ranging from acquisitions and dispositions to securitization of real estate properties and portfolios to entity-level mergers and acquisitions. We believe that our experience and knowledge can help you successfully address today's challenges while preparing for tomorrow's opportunities.

Contact us

Mark Poen
T +31 (0)6 20 44 53 30
poen.mark@kpmg.nl

Sander Grunewald
T. +31 (0)6 50 69 20 13
grunewald.sander@kpmg.nl

Paul van Iterson
T +31 (0)6 46 74 86 35
vaniterson.paul@kpmg.nl

cyber.kpmg.nl

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.