Deloitte.

Evolving cyber risk in commercial real estate

What you don't know can hurt you

Deloitte Center *for* Financial Services

"In the pace of today's climate, organizations cannot afford to slow innovation simply because it cannot be perfectly secured. But addressing those risks through a program to become secure, vigilant, and resilient is an essential component in achieving strategic and business performance objectives."

- Ed Powers, national managing principal, cyber risk services, Deloitte & Touche LLP

Contents

Cyber risk in real estate—Yes, there is!	2
CRE technology use is broadening the attack surface	3
Many CRE companies are inadequately prepared for cyberattacks	6
Making CRE IT systems secure, vigilant, and resilient	7
Cyber risk management is a growing business imperative	10
Methodology and endnotes	11
Contacts	13

Cyber risk in real estate—Yes, there is!

Retail, travel and hospitality, and the financial services industries have been plagued with cyberattack incidents. In contrast, the commercial real estate (CRE) sector considers itself to be relatively less at risk from a potential cyberattack. This is because CRE firms typically maintain relatively less consumer personally identifiable information (PII) and valuable intellectual property (IP) directly on their own technology systems.

With that said, let's consider an example that illustrates how cybersecurity concerns for CRE companies may be more complicated than generally assumed.

Wendy works as a relationship manager with a bank and recently moved from Boston to the bank's Chicago office. She initially stayed at a hotel and used her corporate credit card for payments. Wendy then leased an apartment through an online rental website, and shared her requisite personal details for purposes of the lease through a secured network offered by the owner of the property. It was a convenient and smooth leasing process.

Wendy also uses the 'passport' option on her phone to store all of her personal details (credit card, insurance details, social security number, etc.) and passwords. During the first two weeks in her new location, she visited different retail stores to buy several essentials to furnish her new home. As she shopped, Wendy used a combination of debit and credit card contactless payments for all her purchases, using the details stored in her phone.[1] Does Wendy realize that her payment card details could be accessed in multiple ways, including through retail-store owners' building management systems?

Wendy loves her new office. The branch has been completely refurbished and uses advanced building technology, with energy efficient and automated control systems that customize the lighting and air conditioning, as preferred by the people on each floor. Wendy's PII data, such as employee number, bank account, and contact details, are stored in the bank's systems, which are now potentially also accessible through the real estate owner's IT systems that include the advanced building management systems (BMS). The interconnectivity between the bank and real estate owners' systems is necessary to facilitate active management of the bank's leased office space. Wendy also uses her ID card, contact numbers, as well as emergency and medical information to access the branch building. Are Wendy and/or the bank aware of the interlinkage of the IT systems with the building owner's BMS, and vice versa?

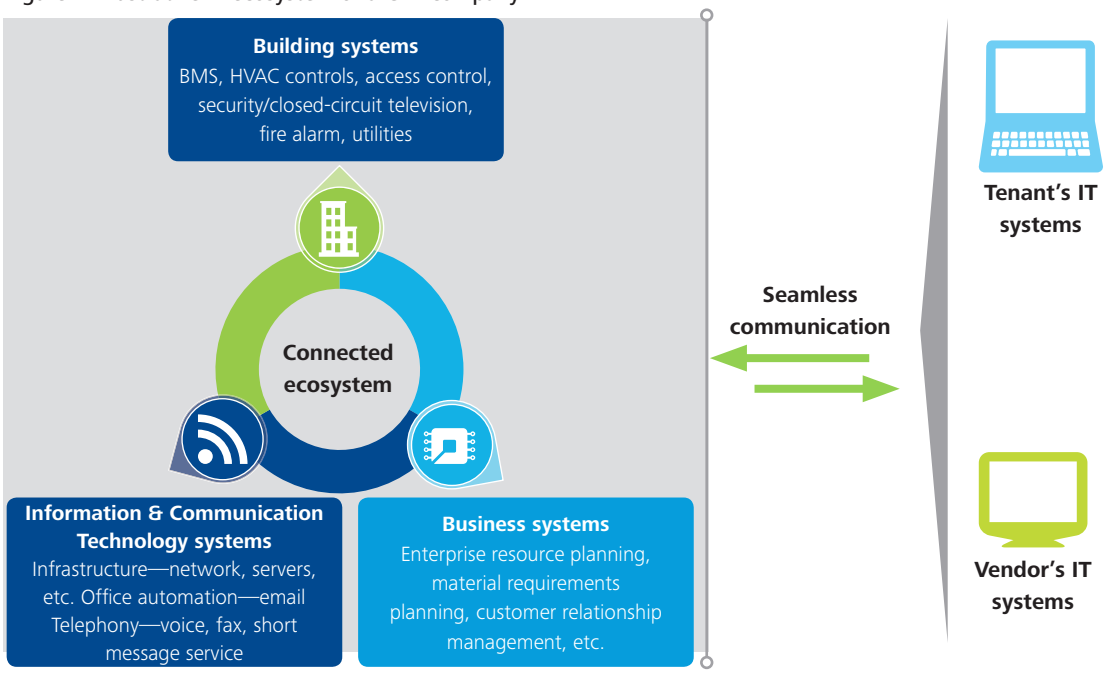
Technology-driven innovation is the order of the day, and more often than not, also one of the ways firms of all types seek to create competitive differentiation. As CRE companies likewise increase technology usage, they also need to implement appropriate security measures to prevent and mitigate cyber intrusions.

The hypothetical example above shows how hackers can access PII data through multiple entry points and individuals, while property owners and their tenants are oblivious to these breaches. Can hackers attempt to take advantage of the interconnectedness of real estate owners' systems across the various property types and tenant IT systems mentioned above through cyber intrusion? The answer is yes. As the example illustrates, tenants' exposure through their physical space (CRE buildings) can be far greater than it seems, making CRE owners a more integral part of their tenants' supply chain and operating systems. And it is for that reason that the CRE sector is as susceptible to cyber risk as are some of the other sectors making headlines as victims of cyberattacks.

CRE technology use is broadening the attack surface

CRE companies are stepping up their use of new technologies such as cloud, mobile, and social media to drive tenant engagement and operational efficiency. In addition, they are implementing increasingly sophisticated technology solutions for building management. Some of the commonly used solutions of this type include systems to automatically control heating, ventilation, and air conditioning (HVAC), lighting, and/or safety systems. In fact, the US BMS market is expected to grow seven to nine percent annually during the 2014–2017 period, reaching $2.2 billion in annual spending by 2017.[2] This growth is coming, in part, from CRE players that are increasing connectivity with tenants and vendors through integration of building management, communication technology, and business systems (Figure 1). Referred to as intelligent buildings, the converged IT systems allow a comprehensive and real-time view of various facilities and enables better adaptability to the requirements of specific tenants and buildings. The interlinkage with other IT systems aids real-time reporting and efficient portfolio management through better availability of information from various sources at the same time and place.

Figure 1: Illustrative IT ecosystem of a CRE company[3]



Source: The Institution of Engineering and Technology, UK, and Deloitte Center for Financial Services analysis

However, the increased use of digital technologies also exposes information and data through multiple channels. At a corporate level, web-based transactions with tenants and vendors, use of cloud services, the growing use of smartphones and tablets under bring your own device (BYOD) policy, and social media presence create multiple access points for the PII data stored by CRE companies.

At an asset level, the interconnectedness through internet protocol-based networks, HVAC and other industrial control systems, and open Wi-Fi networks increase data vulnerability. Do these asset-level cybersecurity risks solely impact the CRE owners? Not in the least—because intelligent buildings tend to be interlinked with tenant systems, creating exposures to tenants whereby their systems and data can be accessed through the CRE owners' IT systems.

Consider the November 2013 data breach at Target Corporation. In this instance, the hackers were able to find a route through the company's HVAC contractor's systems to steal payment card records and other personal information of nearly 110 million customers.[4] Along with reputational damage, the company reported a gross financial loss of $252 million by the end of 4Q14.[5] The incident highlights that the IT systems of CRE owners can act as an entry point for hackers to access tenant data, and that they are becoming an increasingly integral part of a tenant's supply chain.

Interestingly, cyber intrusions through CRE companies can create additional vulnerabilities beyond information theft, such as impact on productivity, life safety, and protection. Billy Rios, a security researcher with the security firm Cylance, Inc. shared his perspectives in a recent interview "Major financial institutions have told us that if you can vary the temperature by five or six degrees, their computers won't be able to process transactions at the normal rate," because heat tends to degrade computer performance.[6]

The above examples and our analysis highlight the development of an increasingly boundaryless ecosystem within which CRE companies operate, and thus a much broader "attack surface" for threat actors to exploit.

Furthermore assuming that various property types use intelligent buildings, in Figure 2 we have developed an illustrative analysis of the potential increase in entry points for hackers through the interconnectedness of building and tenant IT systems. While all property owners and tenants have some degree of exposure to cyberattack, this and the above examples suggests that hotel and retail property types are relatively more vulnerable.

Figure 2: Broadening attack surface by property type

Systems involved	Owner/ tenant	Owner/ tenant	Owner	Owner/ tenant	Owner/ tenant	Owner
Entry points by property type	**Mobile/web applications**	**Online payments/ point of sale (POS)**	**Industrial control systems/ HVAC/BMS**	**Employee devices**	**Webserver/ network/ cloud**	**Open Wi-Fi access**
Hotel	◑	●	◑	●	◑	●
Retail	◑	●	●	◑	◑	●
Health care	◑	○	●	○	●	○
Multifamily	◑	◑	○	◑	●	◑
Data center	◑	○	●	○	●	○
Office	○	○	◑	◑	◑	○
Industrial	○	○	◑	○	◑	○

● High ◑ Medium ○ Low

Note: High to low is defined by the level of risk exposure for each property type by each entry point.
Please refer to page 11 for the methodology.
Source: Deloitte Center for Financial Services analysis

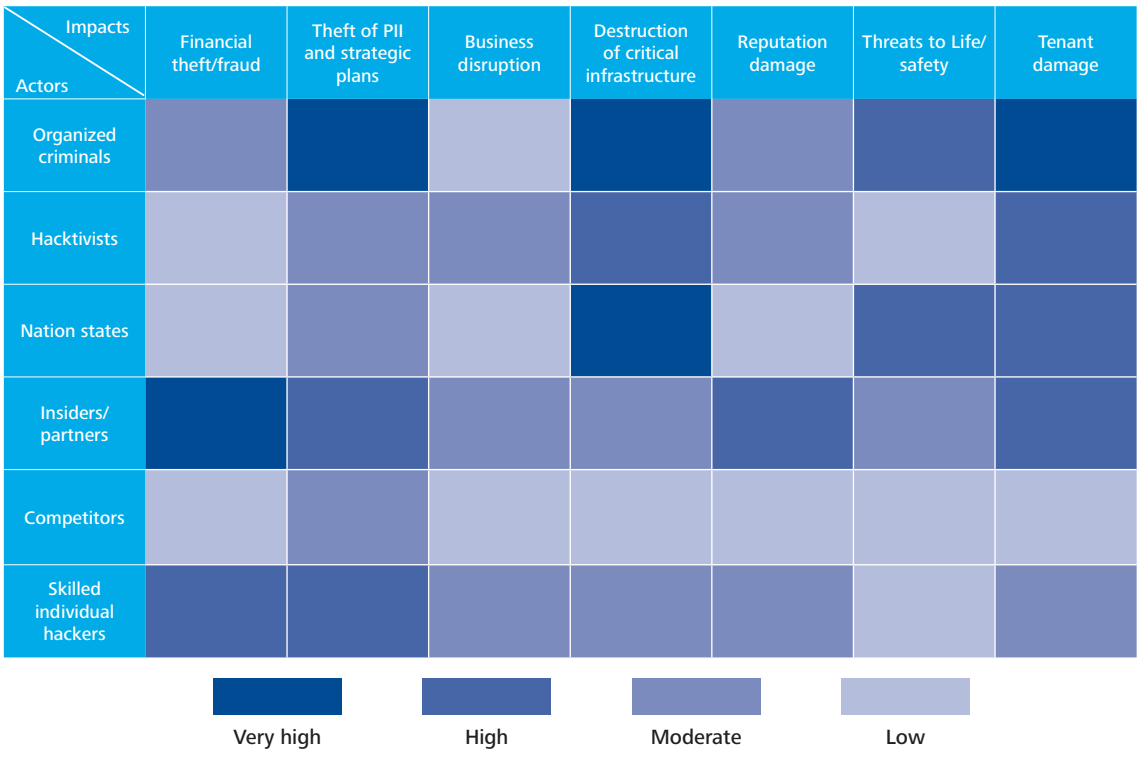
Further complicating the issue, cyber threats are fundamentally asymmetrical risks, meaning that small groups of highly skilled individuals with a wide variety of motivations and goals have the potential to exact disproportionately large and diverse amounts of damage.[7] An illustrative cyber threat landscape (Figure 3) for the CRE sector highlights the need to consider a wide range of actors and motives when designing a cyber risk management strategy.

According to an analysis by Deloitte Center for Financial Services, the most visible objective for cyberattacks on CRE companies has been the theft of PII and other sensitive information, as well as IP, such as strategic plans, engineering drawings, and tenant information. Furthermore, CRE companies may be uniquely vulnerable to treasury management cyber risk, given significant amounts of cash maintained on the balance sheet as well as large dollar transactions related to acquisitions, dispositions, and financing of real estate properties. Many CRE companies have expressed concern about potential cyber vulnerabilities in wire transfer processes associated with these large dollar transactions. Here, we believe that organized criminals and/or insiders could be the most significant potential threat actors. A recent SpectorSoft study suggests that 37 percent of data attacks in the real estate sector are perpetrated through insiders.[8] On a broader level, a Vormetric Data Security study suggests that 93 percent of US organizations feel vulnerable to insider threats.[9]

When it comes to tenants, the interconnectedness of their IT systems with CRE owners' systems as described above, creates several vulnerabilities for them as well. Perpetrators can use the IT systems of the physical asset as an attack surface to cause physical destruction, reputational damage, financial, and/or productivity loss to the tenant. Organized criminals, nation states, hacktivists, or terrorists can destroy critical infrastructure by compromising BMS that can impact both safety of the environment and human life.

In summary, the analysis suggests that the top three risks that the CRE sector should be aware of and prepare for are theft of PII data, an attack on tenants through building systems, and destruction of physical infrastructure. Such attacks could lead to substantial financial exposure, including fines and other costs, revenue loss, decline of shareholder value, and could impact human life and the environment.

Figure 3: CRE cyber threat landscape—a wide range of actors and impacts



Note: The assessment for the first six impact columns assumes CRE players as the primary target of threat actors, and the last impact column assesses cyber threat to tenants in CRE buildings. Please refer to the methodology on page 13.

Source: Deloitte Center for Financial Services Analysis

Many CRE companies are inadequately prepared for cyberattacks

CRE companies are potentially unaware of the data-breach risks from interconnectivity and remote accessibility of building systems and tenant interfaces because, in general, system control and integrity are given more attention than data protection.

Today's building systems fall short of effectively managing any potential cyber intrusion in several areas. For instance, in the past, building systems and protocols were more proprietary in nature, thus presenting entry barriers for hackers. However, newer building systems are more commoditized, using hardware, software, and communication protocols that are more standardized, with known vulnerabilities that hackers can exploit, such as supervisory control and data acquisition (SCADA) systems. Many companies also have insufficient password protection or outdated antivirus and antimalware programs that eventually contribute to heightened cyber risk.

In the financial services industry (FSI), which is the most targeted industry for cyberattcks, the speed of a successful attack is significantly faster than the discovery and restoration time.[10] Similar to the FSI industry, Many CRE companies face big challenges in both detection and response capabilities, which need to be addressed to enhance cybersecurity. Just understanding the modus operandi and extent of damage from a cyberattack can take a significant amount of time.

In late September 2014, a large US real estate investment trust (REIT) discovered that its systems containing PII and key company information had been compromised by a cyber intrusion. Interestingly, the actual breach happened before April 2014.[11] Last year, the company recorded a $2.8 million cyber intrusion expense, including investigative fees and identity protection services.[12] However, the company has yet to fully understand the modus operandi, the exact data that was compromised, and the full amount of damage.[13]

Business leaders indeed acknowledge cyber risk as a growing threat. According to a 2014 Deloitte Business Confidence report, a third of business leaders rate cyber risk as the second highest obstacle to company growth in the next one-to-three years.[14] However, nearly three-quarters of these leaders aren't investing in technology to address cyber risks.[15] Our sense is that a similar case exists in the CRE sector. If nothing changes from the current state, CRE companies are at risk of underestimating cyber threats and may be limited in their ability to respond proactively to these treats.

Making CRE IT systems secure, vigilant, and resilient

Lessons learned from the broader FSI: Key steps taken by a large US bank to be more secure, vigilant, and resilient

The banking sector has been one of the key targets of cyberattacks, given its continuous adoption of new technologies which introduce new cyber vulnerabilities. Take the case of a large bank in the United States which has also been a victim of such attacks, including distributed denial-of-service and data security breaches, which continue to get more complex and sophisticated. Faced with incessant cyber threats, the bank has taken a series of steps to improve its cybersecurity capabilities.

Top management has recognized cybersecurity as a key component of its multiyear technology strategy roadmap and has included cyber risk in its operational risk management framework. Putting policies into action, the bank is making investments annually to improve the overall security of its systems, software, and networks. The bank plans to track all of its internal information over the Internet and centrally monitor its systems. The resulting consolidated view will likely enable the institution to be more vigilant and help identify potential cyber threats to the bank and its customers.

The bank also recognizes that cyber risk is not just direct, but also derived from the third parties with whom it does business, such as exchanges, clearinghouses, and vendors. The bank is therefore collaborating with its business partners to enhance its overall defenses and resilience against cyber threats. All these efforts can be in vain without employee support, as insiders can be the Achilles' heel that hackers can exploit. The bank is spreading awareness and understanding amongst its employees on responsible cyber practices in their day-to-day activities, such as setting strong passwords, updating them regularly, and using only trustworthy software.

Ultimately, the bank acknowledges that cyber risks are evolving in their complexity and impact each day. The institution will need to continuously improve its cyber defenses and be vigilant and more resilient to future cyberattacks if and when they occur.

CRE companies will need to consider a targeted and multipronged approach to manage cyber risk. They need to understand that a cyberattack is an inevitable and imminent threat—the intensity of which may vary based on automation level and tenants' IT exposure, but one that will undoubtedly increase over time. As companies innovate and increase technology usage to enhance competitiveness and operational efficiency, they should pay equal attention to data protection and security. It is important to note that an effective plan should include an approach to improve the ability to be secure, vigilant, and resilient (Figure 4), as these concepts are the cornerstone of any cyber risk management strategy.

Enhancing *security* through a "defense-in-depth" strategy[16]

A good understanding of known threats and controls, industry standards, and regulations can guide organizations to secure their systems through the design and implementation of preventative, risk-intelligent controls. Based on leading practices, CRE companies can build a defense-in-depth approach to address known and emerging threats. This involves a number of mutually reinforcing security layers, both to provide redundancy and potentially slow down the progression of attacks in progress, if not prevent them.

Increasing *vigilance* through effective early detection and signaling systems[17]

Early detection, through enhancement of programs to detect both the emerging threats and the attackers' moves, can be an essential step toward containing and mitigating losses. Incident detection that incorporates sophisticated, adaptive signaling and reporting systems can automate the correlation and analysis of large amounts of IT and business data, as well as various threat indicators, on an enterprise-wide basis. Similar to financial services firms, CRE companies' monitoring systems should work 24/7, with adequate support for efficient incident handling and remediation processes.

Improving *resilience* through simulated testing and crisis management processes[18]

Resilience may be more critical as destructive attack capabilities gain steam. CRE companies have traditionally planned for resilience against physical attacks and natural disasters; cyber resilience can be treated in much the same way. Companies should consider their overall cyber resilience capabilities across several dimensions. First, systems and processes can be designed and tested to withstand stresses for extended periods. This can include assessing critical online applications for their level of dependencies on the cyber ecosystem to determine vulnerabilities. Second, CRE companies can implement playbooks to help triage attacks and rapidly restore operations with minimal service disruption. Finally, robust crisis management processes can be built with participation from various functions including business, IT, and other areas within the organization.

In our view, there are four steps that companies should consider to be secure, vigilant, and resilient (Figure 4):

Elevate cyber risk as a strategic issue:

The pervasiveness of cyberattacks is well-established by now. The initial step for CRE c-suite leadership is to acknowledge cyber threat as a strategic issue that requires both the board's attention and involvement of senior executive leadership, rather than as a mere IT or operational issue. Additionally, the board and/or executive management also needs to determine responsibility and accountability for cyber risk management. Given the boundaryless nature of a cyberattack, CRE boards can potentially benefit from developing a governance model that is adopted by the management team. In addition, there should be at least one senior executive at the helm who is able to lead in a crisis, and also guide the program and enlist collaboration across diverse functions.

Develop policies and frameworks:

Once the board determines the cyber risk governance framework, the next step is to develop appropriate cybersecurity policies and frameworks. These policies essentially set the direction, purpose, and risk appetite for the program by appropriately mapping threats to assets. For this, the chief information officer or other senior technology leader should collaborate with business leaders to develop an understanding of threats, tactics, and practices of an attacker in context of the latter's businesses. Companies may benefit from a gap analysis between the current state and expected security control measures.

CRE companies can also consider leveraging the US government's Cybersecurity Framework. Developed by the National Institute of Standards and Technology, it references globally recognized cybersecurity standards and aims to guide every organization, irrespective of size and complexity, to apply cyber risk management principles and adopt leading practices to improve the cybersecurity of critical infrastructure.[19]

According to Carey Miller, director, cyber risk services, Deloitte & Touche LLP, "implementing the framework should give owners and operators a clearer idea of their cyber risk profile. Armed with that knowledge, they can make more informed risk management decisions and proactively identify the steps required to reduce threats and achieve their cybersecurity risk management goals."[20]

Invest in effective implementation:

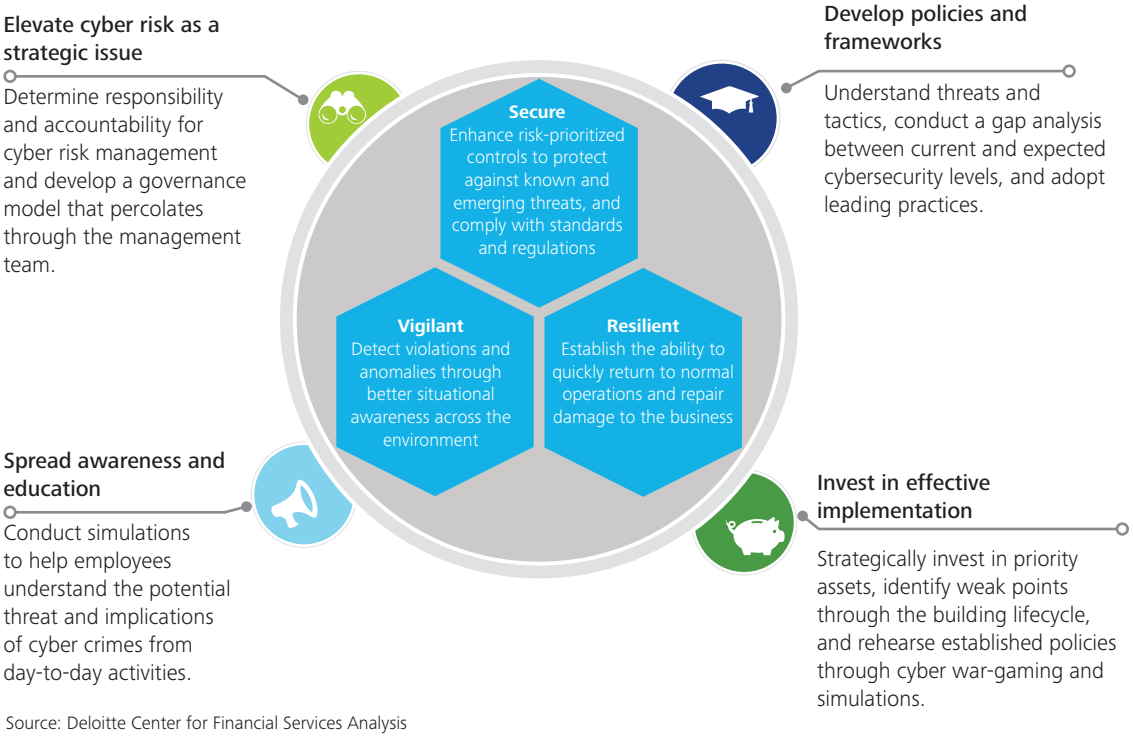
Once CRE companies draft their cyber risk policies, they need to invest in and implement the appropriate security and control systems. While it is not possible to completely eliminate cyber incidents, companies should strategically invest in priority solutions with a focus on gaining intelligence about potential threats and appropriate response management tactics.

Spread awareness and education:

CRE companies should create awareness within the organization about cyber risk and ways in which existing organizational policies and practices could contribute to that risk. Companies can conduct simulations to help employees understand the potential threat and implications of cyber crimes from day-to-day activities, both internal and external. In addition, driving behavioral change within the organization, potentially through rewards and recognition for employees embracing and demonstrating the expected changes, can be a leading practice.

CRE companies also need to be aware of and consider the tenant perspective while planning and implementing their cyber risk processes and controls. As highlighted earlier, property owners have to be increasingly aware that their tenants' information is potentially exposed through the interconnectedness of IT systems. This creates a shared responsibility across two often culturally and technically different companies. A malware incident on a tenant's computer could have a significant impact across the intelligent building, and vice versa. The Department of Homeland Security suggests collaboration between CRE owners and their tenants to manage building-level cyber risk: "leases are the primary mechanism for defining what duties facility owners and operators are required to execute versus the obligations of the building tenants."[21]

Figure 4: Cyber risk management strategy



Source: Deloitte Center for Financial Services Analysis

Cyber risk management is a growing business imperative

The increased use of BMS and intelligent buildings is adding layers of complexity in the CRE business and changing owner-tenant dynamics. This requires companies to potentially lose their false sense of security and make appropriate investments in cybersecurity. CRE companies will benefit from understanding and re-evaluating current security and privacy practices. One of the predominant changes is the need for increased collaboration with tenants and other stakeholders, both internal and external, to improve system security.

CRE Companies need to recognize that it may not entirely be about the ability to prevent cyberattacks, but more about the level of preparedness to quickly respond and limit the damage from a cyber incident. CRE Companies should instill and maintain discipline in adhering to their risk-governance framework and policies. They are likely to benefit from continuous monitoring of the evolving threat landscape, and from adopting a nimble approach toward managing cyber risk. As the cyber threat landscape evolves, there may be increased pressure and a mandate to make appropriate disclosures about cyber incidents in the future. For now, per a 2011 Securities and Exchange Commission directive, companies are advised to disclose information on cybersecurity risks and incidents.[22]

According to Ed Powers, national managing principal, cyber risk services, Deloitte & Touche LLP, "Senior executives should consider the direct link between innovation and cyber risk. The very things organizations do to gain market distinction or drive operational efficiency tend to augment or introduce new cyber risks. In the pace of today's climate, organizations cannot afford to slow innovation simply because it cannot be perfectly secured. But addressing those risks through a program to become secure, vigilant, and resilient is an essential component in achieving strategic and business performance objectives."[23]

Methodology and endnotes

Methodology

Analysis behind Figure 2: Broadening attack surface by property type

The analysis is based on:

- Publicly reported examples of cyberattacks related to each property type and each entry point
- Nature of tenant business and end-customer under each property type (e.g., mall owners have retailers as tenants with consumers as end-customers)
- Our assessment of the cyber susceptibility of each property type through each entry point is based on vulnerabilities that are created by the use of new technologies. The interconnectedness of the IT systems creates additional opportunities for hackers to attack tenants. For instance, retail properties will have a relatively higher cyber risk as their tenants manage large amounts of customer data, which can also be accessed through the owners' BMS due to higher interconnectivity. Our assessment of higher vulnerability for retail and hotel properties is also validated by Verizon data based on actual cases, which highlights that for the private sector, the retail and hotel sectors had the second and third highest number of data loss incidents analyzed in 2013[24]
- We have also considered the vulnerability arising from tampering with the BMS, such as changing the temperature and lighting of a physical space using the central control systems that can lead to productivity and financial losses, among other things

The entry points are categorized based on our understanding of the potential attack vectors and the likely involvement of the IT systems of the CRE owners and their tenants.

Proprietary front-end mobile/web applications: These include the entry points created through the front-end mobile or web-based applications used by owner/tenant. For example, applications introduced by hotel operators and mall owners to provide different services/deals and track customers, respectively.

Online payments/POS: These include entry points wherein the owner/tenant allows online payments or uses POS systems. For instance, hotel operators and retail tenants use these kind of payment channels and are victims of cyber intrusion through these channels.

Industrial control systems/HVAC/BMS: These include entry points enabled by the advanced and more interconnected building technologies used by property owners. For instance, hackers are increasingly exploiting more interconnected and less secured HVAC systems to gain access to key business systems, especially for the retail property type.

Third-party applications used on employee devices: These include entry points created through owner/tenant employees' personal devices, especially in cases where BYOD policies are in place. For instance, many hotel employees use BYOD extensively and use their personal mobile devices to accomplish regular tasks such as submitting expense reports and updating sales numbers.

Web server/network/cloud: These include the entry points created through compromise of owner/tenant networks and servers, apart from web applications and online payments. Data centers are one of the more vulnerable property types in this category due to their network connections and the servers they manage.

Open Wi-Fi access: These include entry points created by open Wi-Fi provisions by property owners. For instance, free Wi-Fi provided at hotel properties is a key entry point that hackers have targeted to get hold of names and credit card numbers of hotel guests. The risk from this entry point will be lower for property types such as offices, which provide a secured Wi-Fi access, except in instances of open guest Wi-Fi access.

Note—high to low is defined by the level of risk exposure to each property type by each entry point.

Analysis behind Figure 3: CRE cyber threat landscape—a wide range of actors and impacts

The analysis is based on:

- Currently reported cyberattacks involving CRE
- Our assessment of potential cyber risk for CRE players, taking into account the relative threat from each actor and their key motives with the maximum impact
- Deloitte's proprietary cyber risk heat maps on different tenant industries

Let us take an example of one threat actor—organized criminals. These are organized groups who largely aim to steal PII and IP of CRE players, destroy critical infrastructure, or inflict some kind of damage to a CRE owner or tenant.

For purposes of this analysis, we have assessed the impact of a variety of cyberattacks at two levels—owner and tenant. We have evaluated the potential impact on tenants due to the interconnectedness with the CRE owners' IT systems, primarily BMS.

Endnotes

[1] Contactless payment systems are credit cards and debit cards, key fobs, smartcards or other devices that use radio-frequency identification for making secure payments, Wikipedia.org.

[2] "US Building Automation Market Primed for Growth," *Electrical Construction and Maintenance*, January 17, 2014.

[3] The constituents of building systems, ICTs, and business systems are referenced from The Institution of Engineering and Technology, UK.

[4] Antonio Olivero, "Top House Democrats Call for Investigative Hearing on Target Breach" American Banker, January 14, 2014.

[5] Target Corporation, "Target Reports Fourth Quarter and Full-Year 2014 Earnings," press release, February 25, 2015.

[6] Rachael King, "Cyber Attackers Target Building Management Systems," CIO Journal. (blog), blogs.wsj.com, April 5, 2013.

[7] "Transforming Cybersecurity: New Approaches for an Evolving Threat Landscape," Deloitte Center for Financial Services, February 2014.

[8] "SpectorSoft 2014 Insider Threat Survey," spectorsoft.com.

[9] "2015 Insider Threat Report," Vormetric Data Security, January 9, 2015.

[10] "Transforming Cybersecurity: New Approaches for an Evolving Threat Landscape," Deloitte Center for Financial Services, February 2014.

[11] Essex Property Trust, Third quarter 2014 earnings call, October 31, 2014.

[12] Ibid.

[13] Essex Property Trust, 10-Q, SNL, November 11, 2014.

[14] "Deloitte Business Confidence Report 2014: The Gap Between Confidence and Action," October 2014.

[15] Ibid.

[16] "Transforming Cybersecurity: New Approaches for an Evolving Threat Landscape," Deloitte Center for Financial Services, February 2014.

[17] Ibid.

[18] Ibid.

[19] Framework for Improving Critical Infrastructure Cybersecurity, NIST, February 12, 2014.

[20] "NIST Cybersecurity Framework: 4 Steps for CIOs," CIO Journal., deloitte.wsj.com, January 14, 2014.

[21] "Commercial Facilities Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan," Department of Homeland Security, 2010.

[22] "CF Disclosure Guidance: Topic No. 2," US Securities and Exchange Commission, October 13, 2011.

[23] "With Cyber Risk, Secure, Vigilant and Resilient Are the Watchwords," Risk & Compliance Journal, Deloitte-WSJ, August 25, 2014.

[24] "Verizon 2014 Data Breach Investigations Report.

Contacts

Industry leadership

Bob O'Brien
Vice Chairman and Partner
Global and US Deloitte Real Estate Leader
Deloitte & Touche LLP
+1 312 486 2717
robrien@deloitte.com

Deloitte Center for Financial Services

Jim Eckenrode
Executive Director
Deloitte Center for Financial Services
Deloitte Services LP
+1 617 585 4877
jeckenrode@deloitte.com

Authors

Surabhi Sheth
Research Leader, Real Estate
Deloitte Center for Financial Services
Deloitte Services India Pvt. Ltd.
+1 615 718 8364
susheth@deloitte.com

Saurabh Mahajan
Assistant Manager, Real Estate
Deloitte Center for Financial Services
Deloitte Services India Pvt. Ltd.

The Center wishes to thank the following Deloitte client service professionals for their insights and contributions to this report:

Vikram Bhat, Principal, Deloitte & Touche LLP
Will Herman, Partner, Deloitte & Touche LLP

The Center wishes to thank the following Deloitte professionals for their support and contributions to the report:

Michelle Chodosh, Manager, Deloitte Services LP
Catherine Flynn, Senior Marketing Manager, Deloitte Services LP
Robert Libbey, Manager, Deloitte Services LP
Aditya Muppa, Senior Research Analyst, Deloitte Services India Pvt. Ltd.
Lincy Therattil, Manager, Deloitte Services India Pvt. Ltd.
Lauren Wallace, Lead Marketing Specialist, Deloitte Services LP
Carrie Winell, Senior Manager, Deloitte & Touche LLP
Prasad Yadav, Senior Research Analyst, Deloitte Services India Pvt. Ltd.

Deloitte Center
for Financial Services

The Deloitte Center for Financial Services offers actionable insights to assist senior-level executives in the industry to make impactful business decisions.