Cybersecurity in commercial real estate

Address emerging cybersecurity threats to safeguard smart buildings
usa.siemens.com/CRE

SIEMENS

Abstract

Recent trends underscore the alarming, increasing frequency of cybersecurity incidents for commercial real estate (CRE) owners and operators, and emphasize the need for leaders to fortify their defenses. In this paper, we explore the complexities of cybersecurity in CRE, including security considerations, emerging threats, and the importance of building a strong cybersecurity culture.

Introduction: The importance of cybersecurity to safeguard smart buildings

Commercial real estate (CRE) faces distinct cybersecurity challenges as it embraces digitalization, thus converging operational technology (OT) platforms with information technology (IT) networks. To deliver on the promises of smart buildings, HVAC, lighting, access control, and other OT platforms require constant connectivity via IT networks to bring the physical building space into the digital realm. Yet the fusion of these layers can multiply cybersecurity risks and vulnerabilities by expanding the attack surface as each device, software platform, and piece of equipment becomes connected.

Cybersecurity incidents come at an enormous cost. In the U.S. alone, the average cost of a data breach in any industry has now surpassed $9.36 million, although the true cost may be much higher once you consider damage to an organization's reputation, business downtime, and potential litigation costs.

In the event of an attack, many organizations have obtained cybersecurity insurance, which can help recoup some financial losses. Some organizations, however, have reported that this type of insurance has become more difficult to get; this is partly due to a declining number of providers who will underwrite these policies. More, the level of cybersecurity is higher than ever to be eligible for these policies, and once covered, insurance premium prices are rising.

One side benefit here is that meeting the insurer's requirements can help improve the organization's security posture, which is especially important because obtaining a cybersecurity insurance policy is not a substitute for good cybersecurity practices, training, and culture.

Cybercriminals continually evolve their approach

Cybercriminals increasingly target CRE properties with ransomware attacks, where bad actors shut down a platform like the organization's financial database or building management system and then demand payment to restore access. These attacks can deeply impact essential operations and, unfortunately, continue to grow in terms of both frequency and scope; recent industry data estimates that there's a new attack every two seconds, and it will ultimately cost victims $265 billion every year by 2031 .

At the same time, CRE building owners and managers rely on third-party vendors and service providers for both IT and OT systems. A single security breach at a supply chain vendor could rapidly cascade through connected systems, disrupting operations on a much broader scale.

The impact of AI

The rise of AI-driven attacks is equally alarming. The FBI writes, “AI provides augmented and enhanced capabilities to schemes that attackers already use and increases cyber-attack speed, scale, and automation.” This is especially true for AI-engineered phishing attacks, which can fool even the most well-trained targets, costing the organization in terms of lost revenue, operational downtime, and reputational damage.

Cybersecurity considerations for CRE

Cybersecurity throughout a commercial real estate organization necessitates a comprehensive understanding of both information technology (IT) and operational technology (OT) systems. CRE executives must navigate the complex interplay between these distinct systems. Given their interconnectedness, a breach in one area can have significant repercussions in the other, making a holistic, integrated approach a strategic imperative.

	IT SECURITY **Confidentiality**	**OT SECURITY** **Availability**
Asset lifecycle	3-5 years	10-20 years
Network design	Designed for cybersecurity	Built over years
Flexibility to adapt to emerging concerns	High	Low, function-specific
Uniformity	High	Low, mix of devices and operating systems
Protection approach	Standards-based, defined	Maturing but still ad-hoc

Today's cybersecurity practices often include patch management to help close security vulnerabilities while optimizing software and device performance. Newer IT systems have been designed for this practice, but OT systems usually have much longer lifecycles, sometimes spanning decades. When these devices were created and implemented 20 (or more) years ago, they weren't designed to fight cybercrime; not only were they not built for patch management and other cybersecurity measures, but they may also have vulnerabilities that organizations have not yet considered.

Moreover, OT cybersecurity remains a relatively unknown discipline among CRE owners and operators, and IT cybersecurity defenses are ill-suited to detect anomalies within OT infrastructure. Cybersecurity tools that work well on IT layers must be tailored for OT and deployed in different ways while also developing new protection concepts and approaches sensitive to uptime and availability concerns.

Multi-tenant environments in which each tenant controls their own network infrastructure can create even greater challenges. Although an individual network may not affect the entire building or building portfolio, cyberattacks that target underlying OT platforms, such as the HVAC system, can disrupt the entire facility's operations and tenants' ability to conduct business.

Even standard operating procedures done with the best of intentions can do more harm than good if they're applied without knowledge of the OT environment. Examples are incorrectly applied firewall rules, poor zero trust lists, and even poor scanning for malicious signatures.
It can happen relatively quickly on IT networks and lead OT equipment such as HVAC infrastructure, lighting controls, fire and life safety systems, and surveillance technologies to be inadvertently taken offline, leading to data loss, uptime impacts, or system functionality.

Cybersecurity and tenant retention: protecting operational continuity

For building owners, a stable revenue stream depends on tenant retention. Should a cybersecurity attack within the property disrupt a tenant's operations—whether through halted access to building systems, compromised data, and/or prolonged downtime—tenants may reconsider renewing their leases, viewing the property as unreliable for their business continuity needs. Losing even a single tenant can result in revenue loss and additional expenses associated with vacancy, marketing, and lease negotiation.

This risk underscores the critical need for robust cybersecurity measures. By proactively safeguarding OT platforms as diligently as IT platforms, building owners can help protect their physical infrastructure, shoring up tenants' confidence in the property's long-term resiliency and stability.

Compliance and regulatory landscape

A range of standards and regulations also contribute to CRE firms' cybersecurity journey:

- **ISO/IEC 27001:** This international standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within the context of the organization's overall business risks.
- **NIST SP 800-53:** Developed by the National Institute of Standards and Technology (NIST), this publication provides a catalog of security and privacy controls for federal information systems and organizations in the United States. It helps data centers to assess and improve their ability to prevent, detect, and respond to cyberattacks.
- **PCI DSS (Payment Card Industry Data Security Standard):** This standard applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. It includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measuress.
- **SOC 2 (Service Organization Control 2):** SOC 2 is specifically designed for service providers storing customer data in the cloud, and it requires companies to establish and follow strict information security policies and procedures. Compliance with SOC 2 is often necessary for technology and cloud computing companies.
- **GDPR (General Data Protection Regulation):** GDPR imposes strict rules on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It affects organizations that store or process data pertaining to EU citizens..

In short, the regulatory landscape is complex and continuously evolves, and CRE organizations must stay current with the latest changes and updates in regulations. Complicating the conversation is the fact that these regulations and standards were created primarily to protect sensitive information, and not necessarily with OT devices and applications in mind.

NOTE; The foregoing summary is not intended as nor should be relied upon as legal advice. Consult your legal advisor for specific questions regarding applicable legislation and mandatory compliance measures

Fostering a strong cybersecurity culture

Because human error is often a weak link in cybersecurity, instilling a culture of security consciousness among all staff members by ensuring they are aware of potential cyber threats and the critical role they play in safeguarding the smart building portfolio is essential. By addressing human factor risks, CRE organizations can significantly enhance their overall security posture.

Existing IT training and awareness programs should be updated and adapted to consider the OT environment. A phishing attack, for example, that targets a financial executive will inherently be different than one that targets an OT stakeholder. Tailoring an existing cybersecurity program for the OT environment will help ensure all teams receive relevant training and ultimately drive a broader culture change throughout the organization.

Organizations that encourage a sense of ownership and responsibility for cybersecurity while also establishing clear communication channels for reporting security incidents and concerns may realize greater success in fostering a more resilient and vigilant cybersecurity culture.

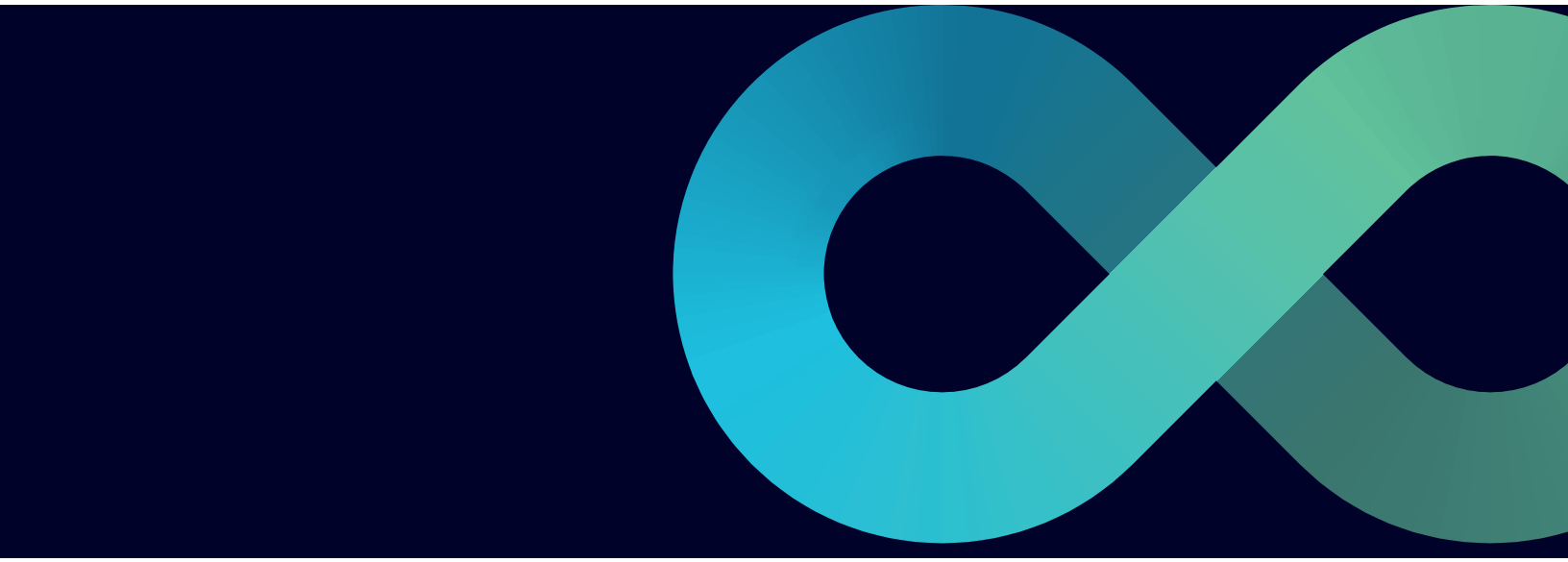
Moreover, one of the most effective ways to ensure robust cybersecurity across IT and OT platforms is by partnering with a cybersecurity provider who has achieved ISO/IEC 27001 certification. This globally recognized standard demonstrates the provider's commitment to implementing and maintaining a rigorous information security management system (ISMS), ensuring that all processes and data handling meet the highest levels of security and compliance. For CRE firms, partnering with an ISO/IEC 27001-certified provider can help mitigate risks by aligning cybersecurity practices with international best practices.

Charter of Trust

The Charter of Trust is an initiative to establish a framework for cybersecurity standards and practices across various industries. Launched by Siemens in collaboration with other global companies and organizations in 2018, it outlines ten principles for improving cybersecurity and building trust in digital technologies.

1. Responsibility of government and businesses to protect critical infrastructure and digital ecosystems
2. Adoption of cybersecurity by design and default in products, systems, and services
3. Promotion of transparency and accountability in cybersecurity practices
4. Assurance of integrity and authenticity in digital products and services
5. Protection of intellectual property and data privacy
6. Establishment of global cybersecurity standards and certification processes
7. Development of cybersecurity skills and competencies through education and training
8. Collaboration and information sharing among stakeholders to address cybersecurity challenges
9. Strengthening supply chain security and resilience
10. Commitment to continuous improvement and innovation in cybersecurity

The Charter of Trust fosters collaboration between industry, government, and academia to address cybersecurity challenges comprehensively. It emphasizes the importance of proactive measures to protect critical infrastructure, promote trust in digital technologies, and help ensure the security and privacy of individuals' data.



Looking ahead: implications for cybersecurity in CRE

As technology advances, so do cybercriminals. CRE organizations must stay informed about the evolving threat landscape so they can prepare for cybersecurity incidents and be ready to defend against a variety of attacks. Consider how today's threats now include AI-driven attacks, which leverage machine learning for more sophisticated evasion techniques. Additionally, the large language models that AI-based tools rely on are especially adept at fueling social engineering tactics. On the other hand, these algorithms are also great for preempting cyberattacks via network canvassing to detect and alert to potential threats.

Regular training, up-to-date security policies, and proactive monitoring are essential, foundational components of a cybersecurity strategy. Threat intelligence and rigorous third-party risk management programs are also essential.

Building owners and operators who have embraced digitalization experience wide-ranging benefits for operational efficiency, tenant experience, and progress toward sustainability objectives. At the same time, owners and technology partners alike must proactively invest in protective measures to help safeguard their smart buildings. Many CRE organizations already turn to Siemens as a trusted partner to help plant, implement, and integrate a tailored cybersecurity program. We have more than 1,300 cybersecurity experts who work to safeguard your smart building infrastructure, and our end-to-end approach means you can rely on a single partner to protect your organization and achieve mission-critical cybersecurity goals. Learn more at **usa.siemens.com/CRE.**

[i] CSOOnline.com | link
[ii] CNBC.com | link
[iii] CybersecurityVentures.com | link
[iv] FBI.gov | link
[v] HelpNetSecurity.com | link

Legal Manufacturer

Siemens Industry, Inc.
950 Deerfield Parkway
Buffalo Grove, Illinois 60089-4513
United States of America

Telephone: +1 (847) 215-1000
usa.siemens.com/CRE

Order No. 153-SBT-774