5 LEADERS ON THE FUTURE OF CYBERSECURITY IN COMMERCIAL PROPERTIES

In conversations with five leading experts in the security space, this Deep Dive explores the challenges, solutions and strategies for strengthening cybersecurity efforts, mitigating risks, and helping property managers safeguard their real estate assets.

BOMA International

CONTENT

By: Ella Krygiel
for BOMA International

BOMA BEST
BUILDING CERTIFICATION PROGRAM

Changing the Future of the Built Environment

BOMA BEST is a series of programs which are both certifications and building management tools. They encourage smart and sustainable solutions for existing buildings, promoting health, efficiency, cost-effectiveness, and low-carbon performance. BOMA BEST certification represents a globally recognized symbol of sustainability achievement and is driving change.

Three BOMA BEST Programs

With three programs and five certification levels, there are several ways for you to set your building on the path to becoming the BEST it can be.

BOMA BEST SUSTAINABLE BUILDINGS
is a certification program and a building management tool that provides a road map on how to decarbonize, reduce water and waste, retrofit for accessibility and equity, and navigate climate risk.

BOMA BEST SMART BUILDINGS
doubles as a management tool, guiding owners and managers on digital transformation within the built environment to optimize operations, drive sustainability, create unique user experiences, and deliver financial value to their stakeholders and customers.

BOMA BEST HEALTHY BUILDINGS
[COMING IN 2024] A program focused on Health and Wellness within the built environment.

Why BOMA BEST?

- BOMA BEST's Framework promotes tenant partnerships, providing data and reports to help management and tenants show ESG commitment to shareholders
- Green-certified buildings have a **13.8% higher resale value** than non-certified buildings
- Green-certified buildings have **7% higher rents** and **3.5% lower vacancy rates**

BOMA BEST office buildings prevented

27,000 tons

of GHG emissions

– equivalent to taking

8,300 cars

off the road for one year

or planting

900,000 trees.

FOR MORE INFORMATION bomabest.org/

APPLY NOW bomabesthub.com/Login

...Cybersecurity is becoming the top priority, often taking precedence over physical security measures.

With cyber threats on the rise and advancements in technology, companies across all sectors are placing increasing emphasis on strengthening their cybersecurity efforts. For many organizations, including those in commercial real estate, cybersecurity is becoming the top priority, often taking precedence over physical security measures.

In Allied Universal's 2023 World Security Report, nine in ten chief security officers (CSOs) from large companies in 30 countries reported greater concern over cyber than physical security. This highlights the critical importance of cyber defenses in today's increasingly digital world.

In interviews with five industry leaders, these experts provide actionable insights into how businesses can fortify their cybersecurity protocols, mitigate vulnerabilities and prepare for emerging threats in the digital landscape. Their perspectives emphasize how organizations can safeguard their assets and ensure resilient, secure environments for the future.

This Deep Dive is divided into three key sections:

- **The Cybersecurity Landscape:** Tackling Modern Challenges
- **AI-Driven Security Solutions:** The Future of Safe, Smart Buildings
- **Building Resilience:** The Role of Data, Certification, and Cybersecurity in Property Value

In conversations with five leading experts in the security space, this Deep Dive explores the challenges, solutions and strategies for strengthening cybersecurity efforts, mitigating risks, and helping property managers safeguard their real estate assets.

The Cybersecurity Landscape: Tackling Modern Challenges

As technology advances, so do the challenges associated with it. Cybersecurity, in particular, has been rapidly growing and shows no signs of slowing down. According to the Fortune Business Insights report, Cybersecurity Market Analysis – 2032, the global cybersecurity market is projected to grow from $193.73 billion in 2024 to $562.72 billion by 2032, with a compound annual growth rate (CAGR) of 14.3%. With this exponential growth, industry experts have identified the key challenges that must be addressed:

1. Design and Security Challenges

According to **Paula Balmori Beltran, Global Director of Security Design and Integration at Brivo and Board President of the Secure Building Council,** "security in buildings is much more than just preventing unauthorized access or protecting against threats. It directly impacts the overall experience, operations, and efficiency of spaces. When we think of security in architecture, it's about more than just setting up locks and cameras—it's about designing spaces that improve how people interact with the environment, optimize operations, and enhance the safety and functionality of the building. For example, understanding how employees move through a building or how people use common spaces can lead to smarter design choices, like reducing costs on amenities that aren't used or reconfiguring layouts for better flow." Building design plays a key role in physical security, and integrating technologies like access control, cameras, and turnstiles takes this further. Research in the Journal of Facilities Management shows that combining these systems improves both security and efficiency by centralizing data and enabling faster responses. For instance, linking access control with video surveillance allows for quicker emergency action. Fastlane Turnstiles highlights that modern turnstiles with biometrics add extra security while blending into the building's design.

2. Cybersecurity Breaches

Rachelle Loyear, Vice President of Integrated Security Solutions at Allied Universal, noted, "If we look at what people said in our World Security Report, and reflect on the key topics of most of this

and reflect on the key topics of most of this year's industry events, we continue to see cybersecurity breaches as a major concern across all sectors. Ransomware, phishing, and malware attacks remain a major source of trouble, with criminals exploiting weaknesses in both cloud and physical infrastructure and using increasingly sophisticated tactics, such as using AI for targeted attacks." These attacks have only increased, as evidenced by a *Check Point* report, which found a 30% increase in Q2 2024 global cyber attacks. Their report finds that, "these cyber attack numbers were driven by a variety of reasons, ranging from the continued increase in digital transformation and the growing sophistication of cybercriminals using advanced techniques like AI and machine learning."

3. Network-Based Attacks

Derek Ommert, Director of Business Development at ASSA ABLOY Opening Solutions, explains, "One of the challenges we're facing today is that cyber threats are becoming more sophisticated. In the past, security focused primarily on guards, gates, and locks. Now, however, attackers are more likely to exploit network vulnerabilities—whether that's through HVAC systems, surveillance cameras, or other networked endpoints. If there's a single weak point in the system—like an unpatched password or outdated software—hackers will find it." When analyzing targets for the biggest cyber-attacks, HVAC systems are often overlooked, a Cyber Insight article describes. For background, HVAC systems that are attacked are integrated with Internet of Things (IoT) devices, which "help operators monitor the environment and adjust HVAC settings accordingly, ensuring comfortable temperatures and proper ventilation." Despite these benefits, the systems are vulnerable as they are often poorly secured, as Cyber Insight's research details, leading many organizations to taking steps to invest in proper cybersecurity measures.

4. Integration

Joshua Rousseau, CEO of Amherst Intelligent Security, observes, "The biggest challenge in the industry isn't just the technology—it's the cybersecurity around it. Many security companies focus too much on physical security, thinking putting cameras everywhere will solve the problem. But cameras alone don't stop crimes. The real challenge is building systems that integrate physical security with the data and cybersecurity infrastructure to ensure that the information is both accessible and secure." Rousseau makes a valid point here – as many articles point out that security cameras, while functioning can deter crime, are not useful when implemented incorrectly. For example, in a *Security.org* article, which weighed the pros and cons of security cameras, their main consensus was that "while functioning security cameras have been proven to deter crime, that's only the case when they function correctly."

5. Self-Management

Justin Stearns, VP, Chimera Integrations, explains, "from a security perspective, one of the biggest mistakes I see is when organizations try to self-manage cybersecurity, much like you wouldn't install your own fire alarm system. If you don't have a dedicated team, hiring a managed security services provider (MSSP) is a must. It's an investment in ensuring you're not exposed to the risks of a breach. It's also crucial to back up your data properly, keep those backups separate, and constantly test your systems—this is critical for preventing ransomware attacks." A managed security services provider (MSSP), as Stearns mentioned, is meant to offer a wide range of services "for specific areas such as compliance, cloud security, and identity and access management," as described by *Cyber Security News*. Their article outlines the benefits of their services to organizations and how they prevent security threats.

With design and security challenges, cybersecurity breaches, network-based attacks, and integration and self-management risks on the rise, organizations must adopt a more comprehensive and proactive approach to securing both physical and digital assets. These key areas are essential to address as the cybersecurity market is expected to reach $10.5 trillion annually by 2025, according to a report by *Cybercrime Magazine*. Below are the solutions or trends that our industry experts believe we'll continue to see:

1. Cloud-Based Access Control

One solution that property managers can consider when tackling these multifaceted cybersecurity challenges is to embrace cloud-based, integrated security systems that enhance both efficiency and protection. **Paula Balmori Beltran** explains that "security, and specifically smart security technology, is influencing building operations" not only to protect people but also to make buildings more efficient and increase property value. She highlights that "cloud-based access control is revolutionizing security systems" by offering flexibility, cost savings, and ease of maintenance, making it an ideal choice for modern properties. This cloud capability allows for real-time updates and seamless integration with other building systems, functioning much like secure app updates on a smartphone. In addition to these features, cloud-based control is mean to create a "single pane of glass" approach (Stearns later describes this as well), which refers to a "unified, centralized

interface or dashboard that provides a comprehensive view of various security systems, tools, hardware, and data sources in one place," according to a definition by *Genea*. They described the advantages of this approach as offering a "comprehensive overview of a facility's security status," which may make things easier for organizations.

On that same note of cloud-based control, **Rachelle Loyear** also points to the cloud, with her suggestion for cloud-based Security Operations Centers (SOCs), as essential for managing security across multiple sites. A security operations center (SOC), for those unfamiliar, is a "facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis," as reported by *Digital Guardian*. "These allow property owners and security teams to manage security remotely," Loyear explains, ensuring timely responses to incidents regardless of location. As organizations grow and face evolving threats, "cloud-based SOCs offer scalability and flexibility" that support quick adaptations. Pairing these centers with mobile apps, which deliver real-time alerts and provide remote access to security systems, further empowers property managers to monitor their buildings from anywhere, enhancing both security and peace of mind.

2. Frictionless Access Experiences

Derek Ommert sees a pressing need for improved key management in integrated systems. In property management, traditional keys "are difficult to track and can easily be lost or duplicated," which introduces security risks. Ommert notes that "electronic credentials—whether physical or mobile—offer a more secure and flexible solution" for managing access. With growing interest in touchless technology, buildings are also beginning to implement frictionless access experiences, where "technology anticipates user actions—like automatic door openings or credential-based access—without physical interaction." There are growing expectations for frictionless access in workplaces, an *IFSEC Insider* report finds. In fact, research from Brivo highlighted that this is due in part to more Millennial and Gen Z individuals joining the workforce. In fact, Brivo's report determined that upwards of "84% of security professionals think user experience is either extremely important or very important to access control." These findings no doubt will contribute to more frictionless access control experiences in the future.

3. Evolved Training for New Systems and Integrations

Joshua Rousseau brings attention to another key consideration for property managers: understanding the complexity of security systems. Coming from a property management background, he observes that "no one really explains how security systems work," and they often fail to meet expectations in emergencies. Rousseau discussed how Amherst Intelligent Security's fully cloud-based solution bypasses local storage, allowing video data to be uploaded directly to the cloud. This change facilitates real-time analysis and instant alerts, ensuring that property managers can retrieve information more quickly and efficiently. Despite many advancements in the era of cloud storage, a report by *Haptic Networks* doesn't think that traditional data storage methods will be irrelevant just yet. As they described, "The journey of data storage is one of continuous adaptation, where understanding the foundations of traditional methods enriches our capacity to navigate the future."

Justin Stearns stresses the importance of converging physical and cybersecurity. He shares an example of a hospital where the facilities management team controlled physical security while IT managed digital credentials, creating a significant risk due to the lack of communication. On the cyber-attack side, the American Health Association determined that healthcare organizations are vulnerable to cyberattacks because they possess so much information like Social Security numbers and intellectual property related to medical research. These incidents are leading many healthcare security groups scrambling to provide the best technology, cyber security protections and on call assistance. To address this particular issue, Stearns' company, Chimera, developed a platform that allows property managers to monitor both physical and cyber security through a "single pane of glass," simplifying oversight and improving response times. Stearns emphasizes that unifying these systems is critical to closing security gaps and responding effectively to incidents.

By implementing these advanced solutions—cloud-based access controls, frictionless access experiences and evolved training for new systems and integrations—property managers can proactively address the growing challenges of cybersecurity, ensuring their buildings are resilient against current and future threats.

AI-Driven Security Solutions: The Future of Safe, Smart Buildings

The integration of Artificial Intelligence (AI) into building security systems is reshaping the landscape of both physical and cybersecurity. AI offers new opportunities to enhance threat detection, operational efficiency, and overall security strategy. As AI technologies advance, they are becoming a key component in the development of smarter, safer buildings.

1. AI in Cybersecurity

AI is playing a pivotal role in transforming the cybersecurity landscape, creating both new opportunities and challenges. According to *McKinsey & Company's* article, The Cybersecurity Provider's Next Opportunity: Making AI Safer, the rapid advancement of AI, particularly generative AI, is significantly altering the way cybersecurity is approached. McKinsey highlights that "the rapid advancement of AI and generative AI is fundamentally transforming the cybersecurity landscape, presenting both opportunities and challenges for cybersecurity providers. As more organizations use AI to enhance their operations, they risk inadvertently introducing new cyber-related threats."

A key concern is the growing cost of cybercrime. McKinsey notes that, "in 2023, the total cost of cybercrime had more than doubled since 2015," underlining the urgency for businesses to strengthen their defenses. While organizations have improved their response times to cyber threats, it still takes an average of 73 days to contain a breach, a figure that demonstrates the ongoing challenges in securing digital environments. AI is revolutionizing threat detection, enabling faster and more accurate identification of potential security breaches. As noted by Statista, the value of the AI cybersecurity market worldwide from 2023 to 2030 shows that AI-powered cybersecurity solutions are expected to enhance "threat detection and vulnerability management," while also accelerating incident response. AI tools, such as those powered by generative AI like ChatGPT, can sift through vast amounts of data to spot unusual behavior and detect malicious activity.

However, the dual nature of AI also presents risks. *Statista* warns that, "generative AI can also be advantageous for hostile actors," potentially creating more sophisticated cyber threats such as phishing and malware. Despite these concerns, AI's ability to identify threats in real-time is invaluable as the need for more robust defenses grows. The AI cybersecurity market, valued at $24.3 billion in 2023, is projected to reach $134 billion by 2030, reflecting its increasing adoption.

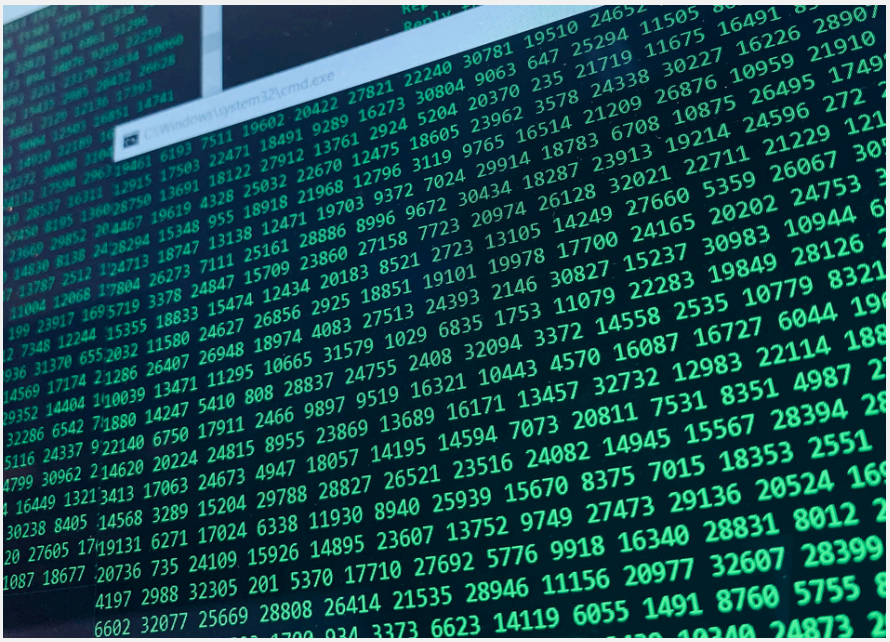
As AI becomes a cornerstone of modern security systems, platforms like IBM WatsonX are setting the standard for AI security. According to IBM, Strengthen Your AI Data Privacy and Security with WatsonX on IBM Cloud, their platform provides comprehensive security measures across all aspects of IT: "IBM WatsonX on IBM Cloud has multi-level security for every aspect of your IT: datacenter, infrastructure, network, cloud, storage, data at rest and transit, and AI models." This ensures that AI models and sensitive data are well-protected, addressing the growing need for robust AI security measures.

2. Cloud Solutions in Modern Building Security

Paula Balmori Beltran highlights the advantages of cloud-based security systems, addressing a common misconception: "One misconception people often have is that cloud-based systems are less secure than on-premise solutions. However, the reality is that cloud systems are often more secure due to rigorous cybersecurity protocols and regulations. At companies like Brivo, cybersecurity has been prioritized from the start, ensuring that any data related to building access and security is well-protected." This point touches on an ongoing debate in the security industry, where opinions are often divided on the benefits of cloud systems versus on-site solutions. For instance, an article by *Cloudwards* noted that 55% of experts believe managing security on the cloud is more complex than on-premises. "However, despite their concern, only 24% of respondents said they had experienced a public cloud-related security incident in the past year." Regardless of whether a property manager opts for a cloud or on-premises solution, it is crucial that they implement a regular maintenance routine and establish precautions to ensure robust security.

Derek Ommert also observes a growing trend toward cloud-based security systems, noting, "A key trend I'm seeing is the shift toward cloud-based security systems. Cloud solutions offer benefits like redundancy, real-time updates, and reduced upfront investment in equipment. However, industries like energy and biomedical sectors remain hesitant to adopt cloud solutions, as they prefer to maintain full control over their data. That said, cloud is definitely gaining traction across the industry, particularly for enterprise-level systems and managed cloud services." Ommert further discusses the increasing use of biometrics, such as facial recognition, for building access, saying, "Facial authentication technology is becoming increasingly common in executive suites, where it's used to facilitate easy access to certain areas like fitness centers. The key is finding the right balance between user convenience and security." Research from Keyless supports the growing

The importance of Artificial Intelligence



preference for biometrics, revealing that 86% of respondents in a poll favored facial authentication over traditional passwords, largely due to its effectiveness. In fact, the study found that "over 131 million Americans use it every day to access their favorite apps, online accounts or devices."

3. Predictive Analytics and Security Integrations

Rachelle Loyear emphasizes the growing complexity of security incidents, noting that "security incidents in 2024 and beyond are becoming more complex and interconnected." She highlights the concerns of CSOs, who warn that economic instability will lead to increased risks such as theft, fraud, and social unrest. To address these challenges, Loyear stresses the need for companies to remain agile, leveraging integrated security systems that unify both physical and cyber security. Her insights align with Allied Universal's 2023 World Security report, which ranked "economic unrest, social unrest, disruption of energy supplies, and threats from war and political instabilities as some of the top anticipated security hazards predicted by CSOs." As we look toward 2025, Loyear believes these threats will continue to dominate the security landscape. She also emphasizes the role of AI and predictive analytics in staying ahead of potential risks: "AI-powered platforms can process data from surveillance systems to detect anomalies and predict potential threats before they escalate," she says. While Loyear acknowledges the value of proactive analytics, she advises that leaders should redefine their goals before trying to adopt 'everything, everywhere, all at once,' ensuring a more strategic and measured approach to security innovations.

4. AI-Driven Video Surveillance

Justin Stearns discusses the integration of AI across both physical and cybersecurity domains: "A major priority for us has been creating a more holistic approach to security by combining both physical and cyber protections. For example, our 911 camera-sharing program enables first responders to get live footage from cameras when an emergency call is made. This is a game changer, especially for schools or any soft target area where fast, accurate situational awareness can save lives." Stearns highlights the shift from reactive to proactive security measures enabled by AI, including real-time intelligence and predictive maintenance: "AI-powered cameras can now detect when a forklift gets too close to a worker or when a dog is present in a building where pets aren't allowed. These systems provide real-time alerts, helping to reduce liability and improve safety for tenants and property owners."

Joshua Rousseau also discusses the development of AI-driven video surveillance: "We developed what we now call a 'video language model,' which is designed to understand video—kind of like large language models used for text data. Our system looks at what's happening across an entire building, drawing connections between cameras, and presenting security teams with only the relevant information—things that need attention. This helps security teams work far more efficiently because they only see events that matter." Rousseau emphasizes how AI can enhance security by providing context to video footage, reducing false alerts and improving operational efficiency.

The advancement of AI-powered cameras in the workforce is designed to help property managers and business owners enhance camera performance and functionality. According to Envysion, these cameras "do more than just record footage," as they are capable of "learning, adapting, and making decisions based on the data they collect." Here are a few key advantages for safety and security that Envysion highlights for those interested in learning more:

1. Behavior Analysis: AI cameras can analyze human behavior patterns, identifying unusual or potentially dangerous activities to enhance overall security.
2. Intruder Detection: Swiftly identify unauthorized access with AI-powered intrusion detection, minimizing the risk of break-ins or security breaches.
3. Emergency Response Enhancement: AI cameras can integrate with emergency response systems, providing real-time information to responders and aiding in swift, effective interventions.

While AI-driven security solutions enhance building protection, building resilience through data, certification, and cybersecurity is equally vital for maintaining property value. The next section will explore how these elements strengthen security and drive long-term value for property owners.

Building Resilience: The Role of Data, Certification, and Cybersecurity in Property Value

As buildings become more interconnected and reliant on smart technologies, ensuring their security has become a multifaceted challenge. Advanced AI, robust cybersecurity practices, and integrated systems are pivotal in safeguarding commercial properties. Insights from industry leaders highlight how certification, AI-driven technology, and a deeper convergence of cyber and physical security are shaping the future of building security.

1. Certification and Standardization as Competitive Advantages

According to **Paula Balmori Beltran**, certification is becoming crucial for building security, much like sustainability certifications in real estate. "More and more, developers and owners are realizing that to stay competitive, they need to prove that their buildings are secure," she explains. "This is where certifications, like those we're developing at the Secure Building Council, come into play. They ensure that the necessary systems and protocols are in place."

The *Secure Building Council* offers the SHIELD certification program, which allows building owners to showcase their adherence to industry best practices in building design, construction and maintenance, while promoting crime prevention and resilience against man-made threats. However, numerous other certification programs are also available, including a recent Forbes article that highlights ten different programs professionals can pursue to enhance their expertise.

2. The Deepening Convergence of Cyber and Physical Security

The connection between cyber and physical security is becoming more pronounced, especially as buildings transition to cloud-based infrastructures. **Rachelle Loyear** points out that "the connection between cyber and physical security will deepen, with AI-driven technology increasing in importance, especially as buildings transition to cloud-based infrastructures."

JLL's research in Cybersecurity in the era of smart buildings, echoes Loyear's perspective, highlighting that "within a typical office building, you've got maybe 20 independent networks vulnerable to hacking…with only five or six highly secured." Loyear's approach, advocating for AI-driven technology to unify security measures across networks, aligns with JLL's recommendation to "hardwire buildings and segregate BAS and subsystems to reduce vulnerabilities." As Loyear sees it, enhancing these connections through AI integration will yield buildings that are both secure and operationally efficient.

3. Leveraging AI for Seamless Data-Driven Integration

Derek Ommert points to AI's transformative potential in integrating security systems across multiple building touchpoints. "There's a growing emphasis on integration, with access credentials used across multiple touchpoints, from parking garages to elevators," he explains. "These seamless, integrated systems not only streamline operations but also provide valuable data on occupancy and movement patterns. This data drives insights into energy use, occupancy, and even HVAC adjustments, creating a safer, smarter environment."

CBRE's article, Cybersecurity: Fortifying Commercial Real Estate for a Digital World, supports Omnert's emphasis on integration, noting the risks associated with building systems, such as "Wi-Fi networks, card-key access mechanisms, and HVAC systems becoming more susceptible to hacking." CBRE advocates for "effective lifecycle management for hardware, especially in legacy properties," and emphasizes that "system recovery procedures are also key." By enabling real-time data monitoring and optimizing energy use, Ommert and CBRE demonstrate how AI can create a responsive and resilient building environment.

4. Redefining Security Through Infrastructure and Human Awareness

"Cybersecurity is always a hot topic, especially in the context of connected devices like security cameras," says **Joshua Rousseau**. "But the reality is that most security breaches aren't about hacking into systems directly—they're often about exploiting weak points in an organization's infrastructure or exploiting human error."

His insights also align with *CBRE*'s findings on common cybersecurity vulnerabilities in smart buildings, including risks related to human error. CBRE notes in their report that "in response, companies are investing heavily in new information security and risk management technology and services," underscoring the need for organizations to fortify not just their systems but also to educate their employees on avoiding mistakes that might compromise security. As Rousseau adds, "Our goal is to redefine what security means in the modern world. It's about integrating cutting-edge technology with a better understanding of real-time security dynamics."

5. Proactive Measures for IoT and BAS Security

Justin Stearns emphasizes the risks associated with IoT devices in buildings, observing that "with the rise of IoT devices, we're seeing a lot more vulnerabilities across both physical and digital infrastructures." He highlights the importance of proactive security measures, pointing to cybersecurity insurance as one way to manage risk, but notes that "technology itself should be leveraged to enhance security, helping clients proactively reduce liability and protect critical assets."

As *JLL*'s report details, one common hacker tactic is to exploit code weaknesses and human errors, such as email phishing and software vulnerabilities, to infiltrate systems. JLL advises "consulting with cybersecurity experts to install systems that make cyberattacks more challenging" and suggests implementing security solutions like "hardware boxes that add layers to building access systems." Stearns' approach underscores JLL's recommendations to bolster cybersecurity through preventative measures, ensuring that IoT devices, building automation systems, and digital infrastructures remain resilient against both internal and external threats.

The convergence of AI, cybersecurity, and integrated security systems is essential to creating safer, smarter buildings. Industry leaders such as **Rachelle Loyear** and **Joshua Rousseau** emphasize the importance of a robust foundation that connects cyber and physical systems, highlighting how AI-driven technology can fortify security and enhance operational efficiency. **Paula Balmori Beltran** underscores the growing value of certification as a means to prove security standards, ensuring buildings remain competitive in an evolving market. **Derek Ommert** points to AI's potential for seamless integration across various building systems, enhancing both security and functionality through data-driven insights. **Justin Stearns** emphasizes the critical role of proactive measures for securing IoT devices and building automation systems, pointing to cybersecurity insurance and technological innovations as key tools in mitigating risk. These perspectives, alongside research from organizations like the Secure Building Council, highlight the need for a comprehensive, multi-layered approach to building security—one that combines advanced technology, certifications, and human awareness to create resilient, future-proof environments. Together, these insights provide a roadmap for the commercial real estate industry to address emerging security challenges in a highly connected digital world.

ACKNOWLEDGEMENTS

I would like to extend my sincere thanks to the following individuals for their valuable contributions to this Deep Dive:

- Paula Balmori Beltran, Global Director of Security Design and Integration, Brivo and Board President of the Secure Building Council
- Rachelle Loyear, Vice President of Integrated Security Solutions, Allied Universal
- Derek Ommert, Director of Business Development, ASSA ABLOY Opening Solutions
- Joshua Rousseau, CEO, Amherst Intelligent Security
- Justin Stearns, VP, Chimera Integrations

RESEARCH WORK CONTRIBUTING TO THIS PAPER:

1. World Security Report. (n.d.). Retrieved from https://www.worldsecurityreport.com/

2. Fortune Business Insights. (2023). Cyber security market - Industry reports. Retrieved from https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

3.Gorse, C. A., & Emmitt, S. (2006). Building security: The role of design in creating safe buildings. Journal of Facilities Management, 4(4), 314–327. https://doi.org/10.1108/14725960610644483

4.Fastlane Turnstiles. (n.d.). Enhancing security and user experience with integrated systems. Fastlane Turnstiles. Retrieved November 25, 2024, from **https://www.fastlane-turnstiles.com/fastlane-news/enhancing-security-user-experience-integrated-systems/**

5. Security 101. (n.d.). Building design: A key component in enhancing physical security. Retrieved from https://www.security101.com/blog/building-design-a-key-component-in-enhancing-physical-security

6. Checkpoint. (2024, June 29). Check Point Research: Highest increase of global cyber attacks seen in last two years — a 30% increase in Q2 2024. Retrieved from https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

7. Cyber Insight. (n.d.). What is HVAC in cyber security? Retrieved from https://cyberinsight.co/what-is-hvac-in-cyber-security/

8. Security.org. (n.d.). Do security cameras deter crime?. Retrieved from https://www.security.org/security-cameras/deter-crime/

9. Cybersecurity News. (n.d.). MSSP providers: The cybersecurity partners you need. Retrieved from https://cybersecuritynews.com/mssp-providers/

10. Cybersecurity Ventures. (2021). Top 5 cybersecurity facts, figures, predictions, and statistics for 2021 to 2025. Retrieved from https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

11. Genea. (2024). 8 benefits of cloud-based access control systems. Retrieved from https://www.getgenea.com/blog/8-benefits-of-cloud-based-access-control-systems/

12. Digital Guardian. (n.d.). What is a security operations center (SOC)? Retrieved from https://www.digitalguardian.com/resources/knowledge-base/what-security-operations-center-soc

13. IFSEC Global. (2023, April 13). Growing expectation for frictionless access in workplaces, report finds. Retrieved from https://www.ifsecglobal.com/access-control/growing-expectation-for-frictionless-access-in-workplaces-report-finds/

14. Haptic Networks. (n.d.). Cloud data storage methods. Retrieved from https://www.haptic-networks.com/cloud/data-storage-methods/

15. American Hospital Association. (2023, May 9). The importance of cybersecurity in protecting patient safety. Retrieved from https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety

16. McKinsey & Company. (2023, June 2). The cybersecurity provider's next opportunity: Making AI safer. Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer

17. Statista. (2023). Global AI cybersecurity market size. Retrieved from https://www.statista.com/statistics/1450963/global-ai-cybersecurity-market-size/

18. IBM Developer. (2024, June 10). Data privacy and security with WatsonX workloads on IBM Cloud. Retrieved from https://developer.ibm.com/articles/awb-data-privacy-security-watsonx-workloads-ibm-cloud/

19. Cloudwards. (2023, March 29). Cloud computing security: How to protect your data in the cloud. Retrieved from https://www.cloudwards.net/cloud-computing-security/

20. Keyless. (2023, May 19). Facial recognition: Applications, benefits, and challenges. Retrieved from https://keyless.io/blog/post/facial-recognition-applications-benefits-and-challenges

21. World Security Report. (n.d.). Retrieved from https://www.worldsecurityreport.com/

22. Envysion. (n.d.). All you need to know about AI security cameras. Retrieved from https://envysion.com/envysion/all-you-need-to-know-about-ai-security-cameras/

23. Secure Building Council. (n.d.). Secure Building Council's certification page. Retrieved from https://www.securebuildingcouncil.com/certification

24. Forbes. (2024, August 28). Forbes' list of best cybersecurity certifications. Retrieved from https://www.forbes.com/advisor/education/certifications/best-cybersecurity-certifications/

25. JLL. (2023, April 5). Cybersecurity in the era of modern buildings. Retrieved from https://www.us.jll.com/en/views/cybersecurity-in-the-era-of-modern-buildings

26. CBRE. (2023, May 15). Cybersecurity: Fortifying commercial real estate for a digital world. Retrieved from https://www.cbre.com/insights/viewpoints/cybersecurity-fortifying-commercial-real-estate-for-a-digital-world