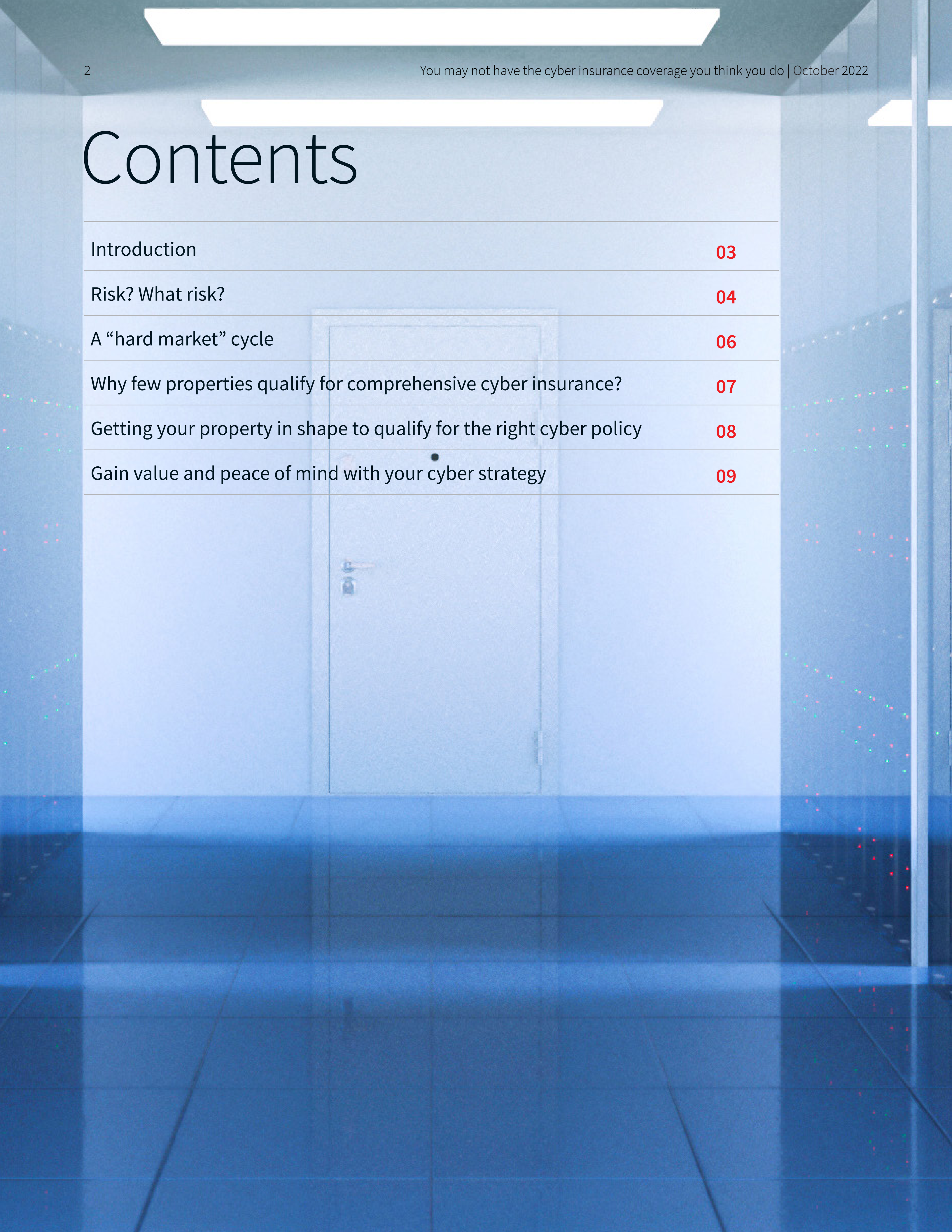
You may not have the cyber insurance coverage you think you do

October 2022



Contents

Introduction

According to a recent report from research firm, Cybersecurity Ventures, cybercrime is expected to account for a loss of $10.5 trillion globally by 2025. To put this figure into context, note that nominal GDP for the entire United States in 2021 was $20 trillion. Thus, considering how massive cybercrime is today, this is a serious risk that must be appropriately addressed. Compounding this problem is a misconception by many commercial building owners and operators that their properties are covered from these types of risks through general commercial property insurance policies. Truth be told, however, is that cyber event inclusions within blanket property insurance policies likely don't provide the necessary breadth of coverage that owners and operators think it does.

These misconceptions are leading to increasingly common situations where property owners believe they are covered when a cyber event occurs - only to find out that this is not the case. This paper will address the risk of Information Technology and Operational Technology (IT/OT) threats to commercial property owners, why comprehensive cyber insurance is one necessary step to better protect against catastrophic loss and suggestions on how to meet minimum compliance and cyber insurance requirements.

Risk? What risk?

Jason Lund, Leader of Technology Infrastructure at JLL, asserts that it's not uncommon for building owners to not fully understand the ramifications of operational technology (OT) threats-or where they sit from an insurance coverage perspective.

"I frequently have conversations with building owners who remain confused about the risk of OT threats and what is or is not covered", states Lund. "In the past, this lack of understanding was not researched sufficiently by the owner. Unfortunately, the problem has now become too great to ignore. Much of what we're doing now is helping our clients think through their OT cyber issues so we can help direct them to providers that specialize in cyber risk mitigation and reduction services. For example, the SEC recently announced it is seeking to hold business leaders accountable for their transparency regarding cybersecurity incidents. This is the type of information we want our clients to know is potentially on the horizon, so they can be prepared for it."

Along with evaluating their current security posture, a second step for owners is to review existing insurance policies with the goal of understanding precisely what level of cyber coverage, if any, is included. This process will help uncover areas where potential coverage gaps exist.

For example, cyber exclusions in commercial property polices may fully exclude a cyber event or limit recovery to specific perils such as fire and explosion. Thus, careful consideration is needed to understand the owner's exposed risk outside of existing policy inclusions. According to Lund, "these exclusions and changes to general property insurance may not be widely known or understood until it's too late".

The introduction of these types of cyber exclusions across commercial insurance policies gained traction in 2017 when NotPetya malware attacks targeted and crippled dozens of businesses, government institutions and critical infrastructures around the world. It was one of the most devastating cyber-attacks in history. Multiple estimates place the global cost of NotPetya to be more than $10 billion.

Because of threats, like NotPetya, and more recently, attacks on popular enterprise software from Kaseya, SolarWinds, Kiteworks/Accellion and others, the traditional property and casualty insurance market has been removing cyber inclusion from these product lines. Part of the reasoning behind this change is that insurers appear to have little to no visibility into what cyber security protections a policy holder has implemented, and the traditional underwriting criteria for a property policy would generally not require this detail. The insurance community at large appears instead to prefer to rely on the expertise within their cyber underwriting teams to assess these risks and provide coverage based on the results of a focused cyber security controls assessment. With this removal of cyber coverage from blanket property insurance policies along with the addition of further contractual requirements for property owners to obtain cyber-specific coverage, the stand-alone cyber marketplace is rapidly growing.

As part of vetting what level of insurance protection a property or campus holds with their existing policies, Joanne Quintal, Cyber Solutions Team Managing Director at professional services firm, Aon, reports “building owners should begin by asking basic policy questions so they fully understand where coverage for their risk is provided from a cyber insurance perspective”. According to Quintal, example questions include:

- What cyber coverage is currently included or excluded within current policies?
- What is the appropriate level of coverage for each property in a portfolio?
- Does the current policy provide coverage for in-building operational technology (OT) as well as information technology (IT) assets?
- What is the expected down time impacting both the physical assets damaged from a cyber event as well as business interruption exposure/loss of rents and extra expense?

Once the answers to these questions are known, it helps make a path to understanding a commensurate level of cyber coverage clearer.

A "hard market" cycle

Simply identifying coverage gaps and seeking to fill them with cyber-specific insurance policies is sometimes easier said than done, however. "A challenge that exists today for securing stand-alone cyber insurance is the fact that this type of policy is coming out of a hard market cycle", states Quintal. "What this means is that based on the rise of cyber claims that have continued to develop from both frequency and severity, insurers have been forced to reevaluate their underwriting results. In a hard market, premium rates go up and coverage reductions/exclusions are added. In this environment, insurers are keenly focused on identifying and evaluating the adequacy of individual cyber security profiles. This investigative work can result in insufficient coverage capacity for a buyer if sufficient cyber security protocols are not in place".

Why few properties qualify for comprehensive cyber insurance?

As mentioned, cyber insurance is coming out of a hard market cycle due to the fact that insurers had limited visibility into a building's IT/OT infrastructure. Additionally, the types of cyber security prevention tools and processes that may be in place were not always understood by the underwriters. The good news is that insurance brokers with financial risk specialists at Aon have resources available to better adapt to new threats and gauge the risk of exposure in advance of a market submission. To accomplish this, however, close collaboration between Aon and the property owner must happen in the first instance. This is so careful evaluation of a property's existing security posture can be appraised to see if it qualifies for more comprehensive cyber insurance.

Underwriters evaluate several key security controls before being able to offer cyber security insurance policies that match appropriate levels of risk between the insurer and property owner. The types of controls that cyber insurance companies are looking for include, but are not limited to:

- Multi-factor authentication (MFA)
- Endpoint detection and response (EDR)
- Patch management
- Secure remote access
- Incident response plans
- Disaster recovery plans
- Backups and email filtering
- Properly architected user management and service accounts
- Phishing and cyber awareness training for all employees

For property owners/operators that are seeking cyber insurance policies to help protect against catastrophic cyber threats, a focus on these specific infrastructure architecture, security and training controls are seen as the optimal path toward reaching qualification status at this time.

Getting your property in shape to qualify for a best-in-class cyber policy

For those concerned about the ability to meet the necessary requirements to obtain cyber insurance, property owners should consult with technology experts that can provide guidance. Dave Cahoon, CTO at Red Bison, a leading company that focuses on implementing and securing intelligent building systems, says "it is important to consult with an expert that understands the unique needs of commercial real estate and how to most effectively mitigate risks that exist within building and campus digital infrastructures".

A holistic approach

According to Cahoon, "The best approach for evaluating the security of your property is to assess all ingress and egress points that communicate within the site. This includes access controls, IOT/OT devices, endpoints, network communications, health and safety, fire controls, BMS and EMS, to name a few. All systems need to be vetted to ensure you are securing the property appropriately and not missing something that could lead to painful issues down the road".

Deploying the right platform

"Properly securing a building starts with the right network platform to serve as a secure foundation", reports Cahoon. "Taking a 'security-first' approach to an in-building network helps to cover all cyber requirements, not just some of them. A modern approach to this problem is to adopt Zero Trust Network Access (ZTNA) models and solutions that not only help to secure operations for existing IT/OT functions – it also collects management and reporting information needed to make sound security decisions in the future. The solution needs to be adaptive and provide proactive security that meets the challenges of an ever-changing threat landscape".

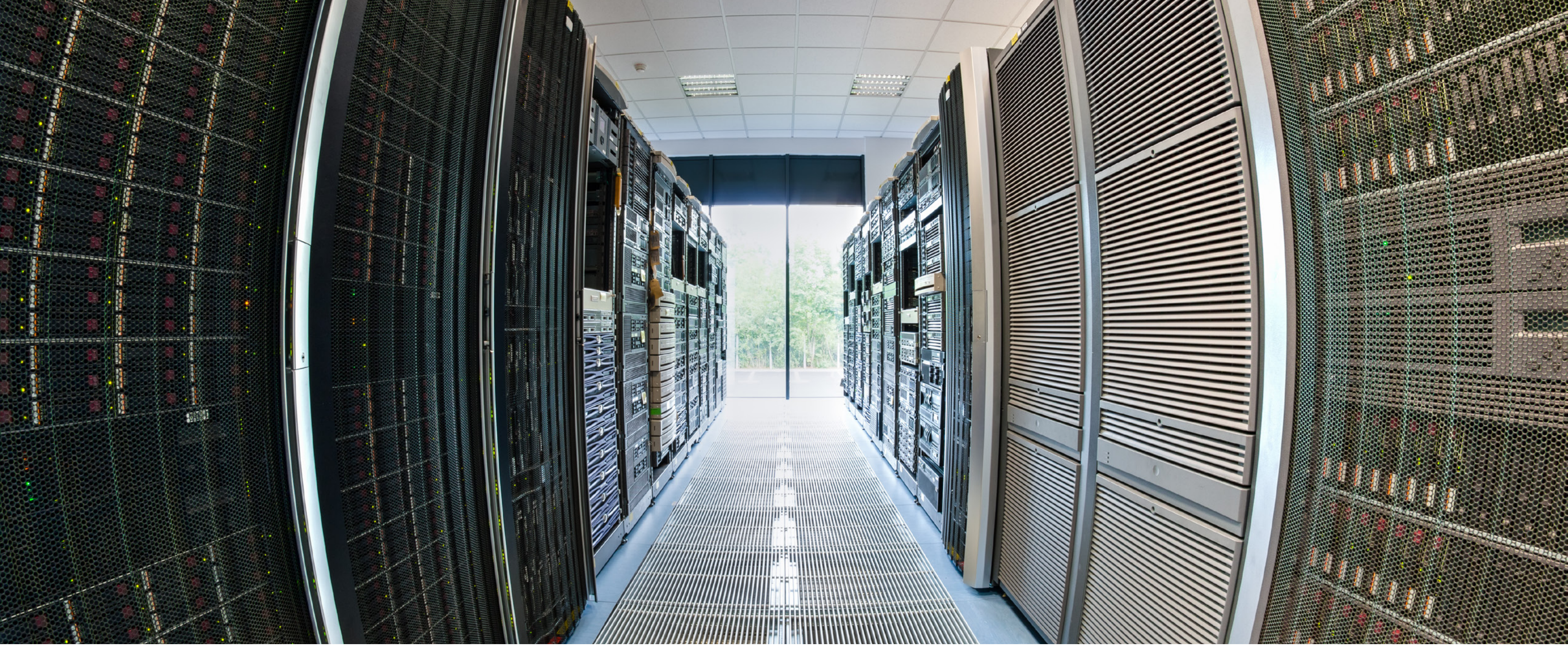
Ease of use and management

Finally, understand that cybersecurity measures like ZTNA should be deployed and managed in such a way as to not impact the usability or manageability of IT/OT systems. Otherwise, you run the risk of impacting digital transformation productivity gains. According to Cahoon, "the goal should be to integrate security tools and processes that are completely transparent from an end-user perspective. That way, you're not impeding a users' or devices' ability to efficiently function on the network".

Cahoon also notes; "It's also critically important to select an intelligent building management platform that offers a single pane of glass to gain important visibility into all your security systems, networks, and endpoints. Doing so allows you to ensure the entire infrastructure is monitored from end-to-end and the architecture provides you the necessary intelligence to easily manage and ensure compliance according to government regulations and for cyber insurance qualification purposes".

Gain value and peace of mind with your cyber strategy

Smart building solutions for both IT and OT use cases help produce impactful economic and intrinsic value when cybersecurity is placed at the forefront. Not only does this line of thinking help prevent cyber-attacks, it also offers a better path toward rapid recovery. This helps a property owner gain access to an appropriate level of comprehensive cyber insurance. In turn, having a cyber insurance policy in place will help to lessen the impact that an attack/breach may have on the digital operations of building owners and occupants.



For more information, please contact:

JLL

Jason Lund
Leader Technology Infrastructure - U.S.
+1 714 657 6401
jason.lund@jll.com

Aon

Joanne Quintal
Managing Director, Property/BI Leader
+1 312 315 8726
joanne.quintal@aon.com

Red Bison

EJ von Schaumburg
SVP of Alliances & Partnerships
+1 973 879 4408
ejvs@redbison.com

About JLL

JLL (NYSE: JLL) is a leading professional services firm that specializes in real estate and investment management. JLL shapes the future of real estate for a better world by using the most advanced technology to create rewarding opportunities, amazing spaces and sustainable real estate solutions for our clients, our people and our communities. JLL is a Fortune 500 company with annual revenue of $19.4 billion, operations in over 80 countries and a global workforce of more than 98,000 as of December 31, 2021. JLL is the brand name, and a registered trademark, of Jones Lang LaSalle Incorporated. For further information, visit jll.com.

About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates.

About Red Bison

Red Bison, a PropTech and Digital Infrastructure Services Company with a highly flexible, vendor-neutral digital platform, simplifies the operations and delivery of advanced technology solutions that improve tenant satisfaction and increase asset values. The Red Bison digital platform seamlessly integrates and connects smart building, BMS, IoT, and other facilities/ management technologies to streamline and fully automate building processes while meeting requirements for increased performance, security, and sustainability.