SECURING YOUR INVESTMENTS IN CONNECTIVITY AND AUTOMATION

cybersmart buildings

EXECUTIVE SUMMARY

THE RISKS AND REWARDS OF SMART BUILDINGS ARE REAL

SMART BUILDINGS are not an option for the 21st Century – they are a necessity. These agile, responsive environments leverage building data to optimize operations and lower facility costs, while increasing safety and sustainability. Smart buildings adapt to occupancy needs in real time, while optimizing energy usage as much as possible. They often connect internal systems – HVAC controls, data networks, power management, etc. – with external networks to more efficiently monitor and manage building operations.

Building owners, operators and managers have traditionally evaluated and purchased smart building capabilities based on business criteria such as functionality, efficiency, cost, reliability and quality. But as you evaluate your next investment, cybersecurity must also be a factor. As access to building data and operational systems increases, so do the challenges associated with securing the smart building environment. The same capabilities that provide beneficial new features – such as remotely accessible performance analytics or carbon-emission monitoring, can also introduce cyber risk to your occupants and your bottom line.

It is no longer enough for a building to be smart – it must now be cybersmart.

"Defending against cyber threats today and tomorrow requires the secure design, development and deployment of building automation systems and controls," said Bill Jackson, president of global products for Johnson Controls, regarding a recently announced partnership with the U.S. Department of Homeland Security on cybersecurity for building automation systems.

Cyber threat actors have demonstrated capability and intent in hacking building automation systems, safety systems and critical environmental technology. Not every connected product is inherently valuable, but accessing a given system can provide a gateway into more sensitive data and systems. For example, hackers have exploited vulnerabilities in HVAC contractor credentials and payment systems as the entry point into a retailers' corporate networks, where they ultimately extracted credit card information. And as the number of sensors and devices talking to one another increases, threat actors can exploit building automation systems to access more data and critical systems than ever before. Data breaches, however, shouldn't be your only concern. Now, as automated systems control more of our environment, there's also increased potential for attackers to create physical incidents through cyber means.

IMPACT FOR PRIVATE AND PUBLIC SECTORS

Corporations and government agencies at all levels – federal, state and local – have taken significant steps to prevent cyber threats to building controls systems. The Unified Facilities Criteria, published by the United States Department of Defense, states: "While the inclusion of cybersecurity during the design and construction of control systems will increase the cost of both design and construction, it is more cost-effective to implement these security controls starting at design than to implement them on a designed and installed system. Historically, control systems have not included these cybersecurity requirements, so the addition of these cybersecurity requirements will increase both cost and security. The increase in cost will be lower than the increase in cost of applying these requirements after design."

by
SEDAR LABARRE and **MATT DOAN**
BOOZ ALLEN HAMILTON

JASON ROSSELOT and **ALEX RUNNER**
JOHNSON CONTROLS

For a complete copy of this white paper, please visit:
johnsoncontrols.com/productsecurity
boozallen.com/cybersmart

HOW CAN KEY BUILDING STAKEHOLDERS SUPPORT CYBER SECURITY?

EXTERNAL STAKEHOLDERS

Building Owner: Advocates for cyber security as a core risk management activity for ensuring a sound investment.

Building Operator: Plays key role in influencing how cyber is integrated into a building management system and its daily operations.

Consulting Engineer: Understands how to integrate security into technical building architecture.

Architect: Uses design role for physical security and safety to determine priorities for cyber-threat mitigation.

General Contractor: Identifies and contracts cyber-ready partners and suppliers for key building technologies.

Integrator: Brings together the proper mix of cyber-ready vendors and partners who can fully integrate diverse building technologies.

Manufacturer: Employs secure product lifecycle across the design, build, distribution, and maintenance of smart building devices and systems.

New Market Player: Introduces feature-laden products and services to smart buildings, but can present real cyber risk if not done thoughtfully.

Occupant/Tenant: Benefits regularly from the features of cybersmart buildings, but must be cautious to not introduce risk through poor behavior.

Visitor: Represents a potential advocate for having a secure experience in a smart building, but can also bring unwanted attention if the experience is subpar.

INTERNAL STAKEHOLDERS

Legal, Safety, & Privacy: Deciphers cyber and privacy requirements for regulatory compliance.

Procurement: Drives the acquisition process in procuring cyber-ready suppliers and vendors.

Marketing & Communications: Carries the cyber message forward to your customers and stakeholders, both internal and external.

Enterprise Risk Management: Guides strategic risk priorities and influences overall cyber investment portfolio.

Finance: Serves as key influencer in prioritizing and guiding fund allocations for security

IT: Brings internal technology to life and is typically the accountable entity for ensuring cyber security is happening across the enterprise.

Audit: Reviews operationalized cyber security compliance against both regulatory and internal policies.

Crisis Management & Business Continuity: Provides a company's backbone capabilities for incident management, including security.

From sci-fi to reality: Envisioning cyber attacks on smart buildings

This new age of connectivity and automation creates tremendous opportunity. Without the proper cyber protections, however, smart buildings can be vulnerable to potential cyber incidents. Risk scenarios include:

1. *Shutting down heating or cooling for sensitive locations, such as pharmaceutical or food processing plants*
2. *Manipulating cooling settings on an HVAC system in a corporate building, creating significant business disruption and lost productivity*
3. *Shutting down cooling or power management functions for a data center, destroying IT equipment and taking business-critical applications offline*
4. *Gaining unauthorized access to an internet-connected physical security system to enable kinetic attacks*

WHAT TO DO?

Yes, the risk is real. But there's no need for security hysterics. There is tremendous business value in embracing building automation—including cost savings, efficiency, and convenience. So don't halt your plans. Instead, protect your investment, and maximize its potential.

A smart approach starts with a strategy and framework to guide consistent actions based on your risk landscape. We recommend five foundational steps to frame the challenge, gain quick wins, and start gaining real traction.

1. OBSERVE AND ORIENT AROUND YOUR SPECIFIC CHALLENGE.

Building operators and managers can learn a lot from military decision-making when it comes to cybersecurity. Out of the gate, when designing infrastructure from scratch or securing legacy building systems, you need to decide which elements of your smart building matter the most. Is it your connected physical security system? What about ensuring continuous uptime of an on-premises data center? You can't afford to secure everything with the highest degrees of assurance, but make sure you prioritize what matters to your business. From here, you'll want to map the available attack surface – take an adversary's perspective and "red team" (i.e., discover) the available pathways to sensitive assets. And to make sure your concerns are justified, roll in some credible cyber threat intelligence that helps you understand the likelihood of different threat actors actually targeting your infrastructure, and how they would do it. Collectively, this systematic process helps you understand what the real cyber risk landscape looks like, and prepares you with a tailored map to take action against.

2. FORGET OLD SILOS—CYBERSECURITY REQUIRES CROSS-FUNCTIONAL TEAMING.

For cyber risks to be well managed, you need involvement and buy-in from across the business. IT, cybersecurity, and facility teams typically have the expertise and the access to take the lead. Working together as one cohesive unit, they also need to coordinate with a range of internal and external stakeholders.

Externally, work with business partners and vendors that materially invest in and value cybersecurity. You need to ensure that you work with trusted partners who are committed to the right policies, products, services and talent. Security can't be an afterthought—it needs to be a primary feature of a third party's stated value proposition.

3. CHANGE THE CULTURE – SPEAK UP FOR CYBERSMART BUILDINGS.

Make sure this issue is heard loud and clear within your leadership community and with internal and external stakeholders. Even with the smartest team, the most expert capabilities, and the most advanced technology solutions, cybersecurity will fail unless you have support from across your ecosystem. Smart building owners, operators, and managers need to build a corporate culture that understands the intrinsic relationship between cybersecurity and the future of your business. Talk to them about the importance of getting this right, including the ROI and their roles in security.

Consider the right mechanisms to engage your senior leaders and your junior staff. Roadshows, risk education, and exercises can help build consensus on opportunity and risk. This is some of the hardest work you'll do, but also the most foundational.

4. BUILD THE RIGHT CAPABILITIES TO ENABLE – NOT HINDER – SMART BUILDING ADOPTION.

You can't just put security technologies in place and claim victory around cyber. Technical solutions are an important piece of the puzzle, but you need to balance deploying technological tools with investments in people and processes.

Incorporate cybersecurity across the smart building lifecycle, being careful not to overburden the process. What core functions will help?

5. GET OPERATIONAL.

Checking the box on today's threat does not mean you're prepared for tomorrow. A compliance-focused approach to all of the above can have detrimental effects if you stop there. You're dealing with an ever-evolving adversary, which means you need a security professional's mindset to defeat them. Your audit team can provide that external assessment of compliance and effectiveness. But your task is to focus on risk and protect your territory. Continually monitor internal and external intelligence to understand your ever-changing risk profile. Find allies — like building controls manufacturers and analytics service providers with a demonstrated commitment to product security—to help you stay ahead. Have a plan, but be prepared to continually evolve. This will help you sleep at night, for years to come.

Applying military-grade security for smart buildings

At federal and military sites, financial institutions, pharmaceutical companies, hospitals, and high-tech companies and labs, low latency and system integrity are paramount. In these environments, deploying a highly secure, hardened network engine is a must.

The Johnson Controls building automation system (BAS) development team saw this need, and got to work with its government and commercial clients to build best-in-class, military-grade security for BAS applications.

The result is the recently released Metasys® secure network automation engine (NAE-S). This new engine provides customers a stronger line of defense against cyber threats to building networks with its new embedded technology designed to shield critical infrastructure against cyber-attacks. Its encryption module encrypts data traveling on the network so that sensitive information cannot be accessed by unauthorized users. This new capability dynamically validates and secures protocol communications. It also secures vulnerable routes in the BAS used to control building operations, providing true end-to-end protection from commonly used hacking techniques.

Lifecycle Phase	Cyber Capabilities and Descriptions	Core Functions Checklist
Acquisition	**Consider Security Requirements.** Include security solutions as part of all specification processes. Work with vendors and technical partners to prioritize security as an integral part of any connected smart building solution. Define how you want the vendor to integrate with your existing network, preferably leveraging a separate network segment for building automation systems. Use system retrofits as opportunities to include the latest security protocols. Be prepared to articulate the budget for security operations throughout the building lifecycle.	□ Security Policy □ Compliance □ Planning & Design
	Assess. Set a consistent assessment framework to evaluate security vendors and their solutions. Favor companies that demonstrate a program that implements secure design and coding practices, and that have a mature vulnerability management program to ensure that product vulnerabilities are discovered, remedied, and patched in a timely manner. Recognize that business imperatives—like cost—may supersede security concerns. So design a framework that evaluates the security implications and tradeoffs of integrations between legacy and new systems, but provides flexibility for add-on security controls you can deploy to help minimize identified risks.	□ Third-Party Risk Management □ Risk Assessments
Deployment	**Build in Security.** Understand vendor recommendations for how to securely deploy building automation systems and work with your IT department to follow those guidelines, and how to add additional controls over and above vendor recommendations based on your compliance and risk needs. Design is important, but how a system is architected and deployed—particularly in the areas of secure network design and remote access capabilities—is critical to monitoring and minimizing your risk.	□ Security Architecture □ Identity & Access Management □ Information Protection □ Secure Product Coding & Testing
Operations and Maintenance	**Update Regularly.** Maintain a software subscription service and preventive service agreement with your integrator. Building controls manufacturers typically "patch forward," so keeping your systems at the latest software revisions is critical to maintaining a cybersmart building. Ensure that you understand how long the vendor will provide security updates and support for the systems, and ensure you have an exit strategy for replacement prior to a system's end of life.	□ Vulnerability Management □ Service Level Agreements
	Test, Monitor, and Respond. Know your risk. Maintain situational awareness on what's connected. Develop and implement an assessment framework that will identify security maturity across all domains in your ecosystem. Diligently and regularly stress-test your assumptions and technical vulnerabilities. Continuously monitor for indicators of an incident. Triage and escalate issues based on a predetermined set of trigger criteria. When needed, lead a whole-of-business response to maintain customer trust as you work with your vendors to deploy the right fixes.	□ Asset Management □ Security Monitoring □ Red Teaming □ Threat Intelligence □ Incident Response □ Exercises

BOOZ ALLEN HAMILTON has been at the forefront of strategy and technology for more than 100 years. Today, the firm provides management and technology consulting and engineering services to leading Fortune 500 corporations, governments, and not-for-profits across the globe. Booz Allen partners with public and private sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cybersecurity, engineering, and innovation expertise.
With international headquarters in McLean, VA, the firm employs more than 22,600 people globally and had revenue of $5.41 billion for the 12 months ended March 31, 2016. To learn more, visit BoozAllen.com. (NYSE: BAH)

JOHNSON CONTROLS is a global diversified technology and multi-industrial leader serving a wide range of customers in more than 150 countries. Our 130,000 employees create intelligent buildings, efficient energy solutions, integrated infrastructure, and next-generation transportation systems that work seamlessly together to deliver on the promise of smart cities and communities. For additional information, please visit http://www.johnsoncontrols.com or follow us @johnsoncontrols on Twitter.