DON'T LET YOUR BAS GET HACKED

The cybersecurity challenge: Ensure Building Automation System data is useful and accessible while keeping it secure.

OSIsoft®

TABLE OF CONTENTS

INTRODUCTION

Today's building automation systems (BAS) face a cybersecurity challenge: Gather, use, and distribute relevant data while keeping it secure. The good news is that commercial and institutional facility data has never been more plentiful, and it is increasingly seen as valuable. The bad news: BAS data and functionality are more vulnerable than ever to being stolen or misused. But there are ways to have your data and keep it secure too.

This eBook explains the cybersecurity risks that facility executives need to be aware of, how those risks have increased in recent years, and how compromised (hacked) data can affect occupants and owners. In the second part, cybersecurity professionals offer insight on how to reduce the risk, and reveal the questions facility executives can ask of their teams and partners to ensure that their systems and data are protected from hackers, saboteurs, and other malicious actors.

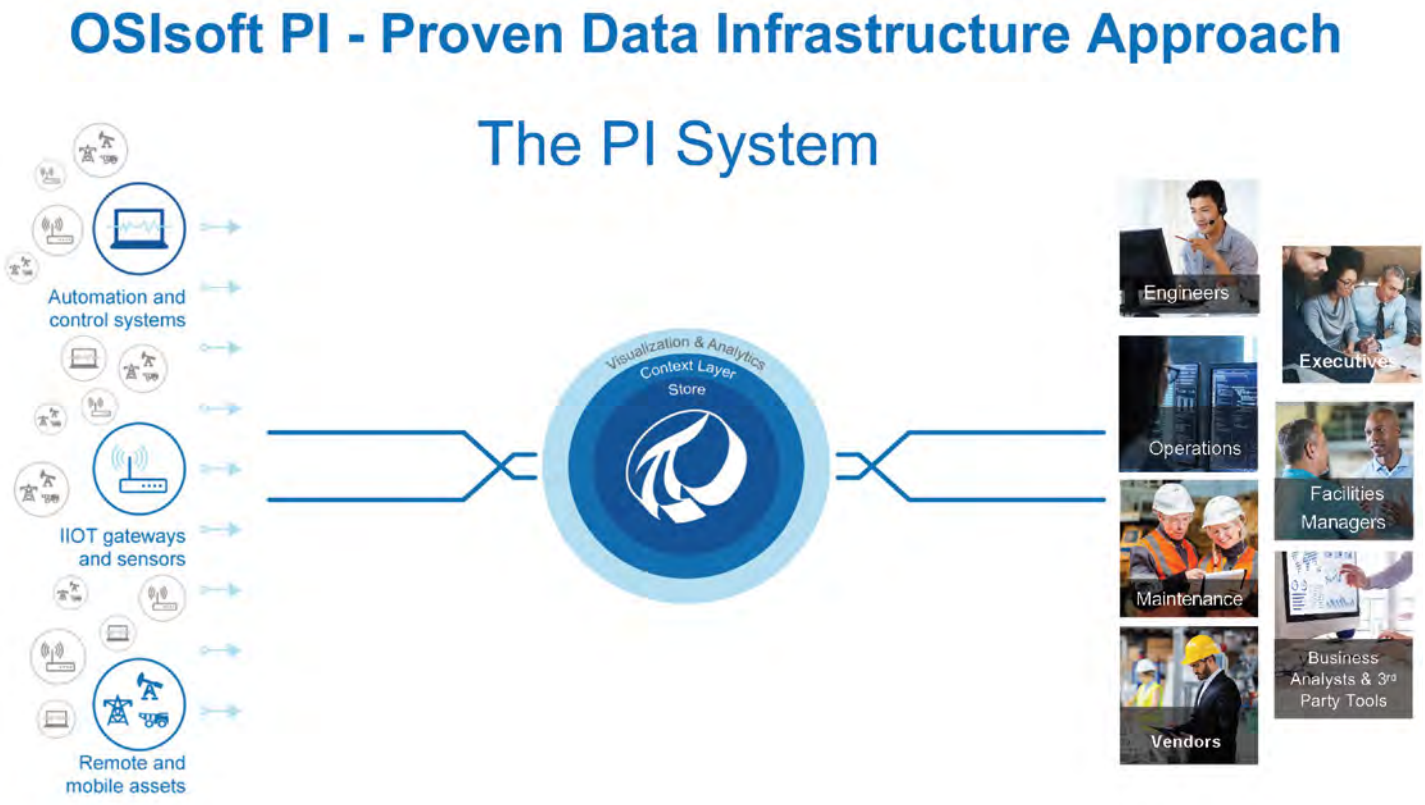
WHO IS OSISOFT?

OSIsoft got its start supplying the PI System, a data infrastructure, to process industries such as oil refineries, power utilities, mines, and manufacturing plants, to support mission-critical operations and decisions through the use of operational data. Its PI System collects, contextualizes, stores and visualizes real time operational data to connect that data to people and tools for insight.

OSIsoft's long experience with industrial cybersecurity enables it to bring the latest knowledge and best practices to facility data.

The PI System organizes and converts raw data streams into meaningful events and values, and it delivers easily consumed data to advanced analytic tools.

When deployed for facility management, the PI System automatically pulls and stores data from many sources across a facility, including building automation systems, energy metering, and building IoT devices. Gathering data automatically is both faster and more reliable than manual data collection, and it better lends itself to real-time analyses and decisionmaking.



The PI System collects data from systems across the portfolio, standardizes and integrates that data, and makes it available to be shared across applications and platforms in a secure manner.

‘IT WON’T HAPPEN HERE’

It’s human nature to think a catastrophic incident like a workplace shooting or weather event “won’t happen here.” The same is true of a cybersecurity breach. No one wants to believe it can happen to them. But just as facility managers have learned the importance of disaster planning and active-shooter drills, they are discovering that BAS cybersecurity and data protection are essential — and not the responsibility of the IT or finance department.

Even if you don’t consider yours a “smart building,” the BAS is just one part of a data-rich and increasingly connected facility. You may have “intelligent” HVAC systems, smart TVs in conference rooms, Internet-connected light bulbs, and other Internet of Things (IoT) devices. Each system, device, or connection is a potential target or tool for a hacker.

Four news items reveal the range and scope of cybersecurity threats to facilities.

GOOGLE AUSTRALIA HEADQUARTERS

In 2013, two security researchers discovered they could hack into the building management system (BMS) for Google’s Wharf 7 office in Sydney, Australia.

The maker of the platform on which the BMS was built had released patches for known vulnerabilities, but Google’s control system had not been patched.

This meant the researchers could discover the system’s generic administrative password (“anyonesguess”) and then access control panels for the HVAC systems. That password also revealed building-specific data, such as blueprints of the floor and roof plans and diagrams of water pipes.

FACILITY MANAGEMENT COMPANY

In 2016, IBM researchers ran a penetration test for a facility management company operating more than 20 buildings around the United States. The researchers found some flaws in the firmware of the building automation system that controlled the sensors and thermostats in one building.

Once the researchers gained access to that BAS, they tried to get into the company's central server. When a layer of protection kept the researchers from accessing the corporate server via the Internet from their physical location, they drove to the company's parking lot and connected to its wireless gateway from there. They then could access the environmental controls for all the buildings that the company managed, including one that housed a data center, which would have allowed them to turn off the cooling system and potentially shut down the servers.

U.S. DEFENSE DEPARTMENT

A 2018 U.S. Department of Defense (DoD) report to Congress estimates it could cost more than $250 million over the next four years to identify, register and implement fixes to vulnerabilities in DoD facility control systems.

The report says it will cost between $11 million and $96 million per military service to complete all requirements laid out in current memorandums and instructions, and "cost estimates will likely increase as more systems are discovered outside of the highest priority systems currently under assessment and remediation."

CASINO OWNER

Also this year, at a Wall Street Journal conference of CEOs, attendees learned how common IoT devices, such as thermostats, refrigeration systems, CCTV cameras, and HVAC systems can make buildings vulnerable to hackers seeking to steal data or disrupt operations.

In one example, the CEO of cybersecurity firm Darktrace said that hackers stole the data related to a casino's best customers by hacking into an Internet-connected thermostat in a lobby fish tank.

The attackers used the smart thermostat to access the casino's IT network. They used the thermostat as a bridge to connect to the WiFi network and extract the data about the high rollers up into the cloud.

WHY CYBER RISK IS RISING

Five trends are increasing the cybersecurity risks associated with facilities operations.

1. EXPECTATIONS FOR DATA ARE INCREASING

That smart thermostat in the casino fish tank is just one example of how almost every physical object is destined to be "smart" and connected to a network. The growing sophistication of consumer electronics means new expectations — and devices — are walking in with employees every day.

Today, occupants and top management are growing accustomed to home automation systems like Nest, Wink, Amazon Echo, or Samsung SmartThings. As a result, they expect the building where they work to be equally smart. They want to be able to adjust conference room lighting or know the energy efficiency of their HVAC system with the tap of a button.

Technology bleeds from the consumer side into commercial and institutional buildings, increasing expectations as it goes.

These expectations add momentum to the move to smarter commercial and institutional buildings, to provide access to data. And with that access come cybersecurity risks because each connected device increases the potential attack surface.

2. THE GROWING VOLUME OF DATA BRINGS A GROWING NEED FOR ACCESS TO DATA.

From pumps and valves to restroom paper towel dispensers, an ever-growing range of building products is gaining the ability to gather and share data. Protocols like BACnet and Modbus connect formerly incompatible building management systems, while Building IoT sensors generate more data than ever before. Access control, water/wastewater processing systems, and computerized maintenance management systems generate still more useful data, as do new technologies like renewable energy systems, energy storage devices, and microgrids.

The value of this data has created a demand for access to it — and opened a door for hackers. It's a conundrum for facility executives.

Access to data is essential for extracting value from that data. The range of analytics available today goes far beyond the capabilities of building automation systems. Data from the BAS can be mined to identify problems that would otherwise go undetected. Building asset data can be combined with other real-time external data or put through algorithms that calculate new data points like Key Performance Indicators (KPIs).

At the same time, demand for data is also growing as top management becomes accustomed to having access to data across the enterprise. Business executives are asking for facilities data as they focus on reducing costs via energy savings, meeting regulatory reporting requirements, or responding to merger and acquisition financial pressures.

The problem with sharing data arises when building control systems lack effective cybersecurity measures, and therefore are vulnerable to being attacked. Each channel over which data is shared, whether across a corporate network or over the Internet, creates potential cyber risks. As demand for access to facility data increases, so do the vulnerabilities.

3. BUILDING SYSTEMS OFTEN LACK GOOD CYBERSECURITY PRACTICES.

Unfortunately, facility cybersecurity practices have not kept up with the rising volume of data. According to facility cybersecurity expert Fred Gordy, BAS were historically installed with convenience in mind. Remote access to systems via a Web browser, for example, could save time and reduce costs for facility executives and their vendors. Security wasn't top of mind, and IT departments didn't have or didn't want to have anything to do with those systems, so they weren't secured. If networks aren't isolated, passwords aren't changed, or other protections aren't layered on, the Internet becomes a channel of risk.

According to a 2016 survey of facility executives conducted by Building Operating Management magazine, just 28 percent of respondents said that they regularly change passwords on all BAS. And only 17 percent described themselves as knowledgeable or very knowledgeable about cybersecurity.

Facility departments today don't often have the situational awareness to know if a system is being inappropriately accessed. In the survey, 35 percent of respondents weren't sure if their organizations had ever detected an attempt to hack into the BAS.

4. BUILDING SYSTEMS ARE NOW SEEN AS TARGETS.

Unlike data from financial systems or voting machines, operational data has historically been viewed as insignificant. That meant the "exposed" building systems of 10 years ago were not as vulnerable because no one was actively seeking them out, and the data they generated was seldom shared or accessed. Today, data is increasingly vital to efficient operations, whether that is the money-saving value of data from energy-management systems or the maintenance value of timely and accurate system information and notification of problems.

Unfortunately, criminal hackers are also discovering the value of stealing operational data outright, or of riding on unsecure operational systems to hijack computing power.

For hackers intent on disrupting normal business operations, access to a maintenance department PC or BAS can disable mission-critical systems and prevent people from doing their jobs. In a high-rise office building, for example, all a hacker has to do to stop business is disable fire control or elevator systems so employees can't occupy the building.

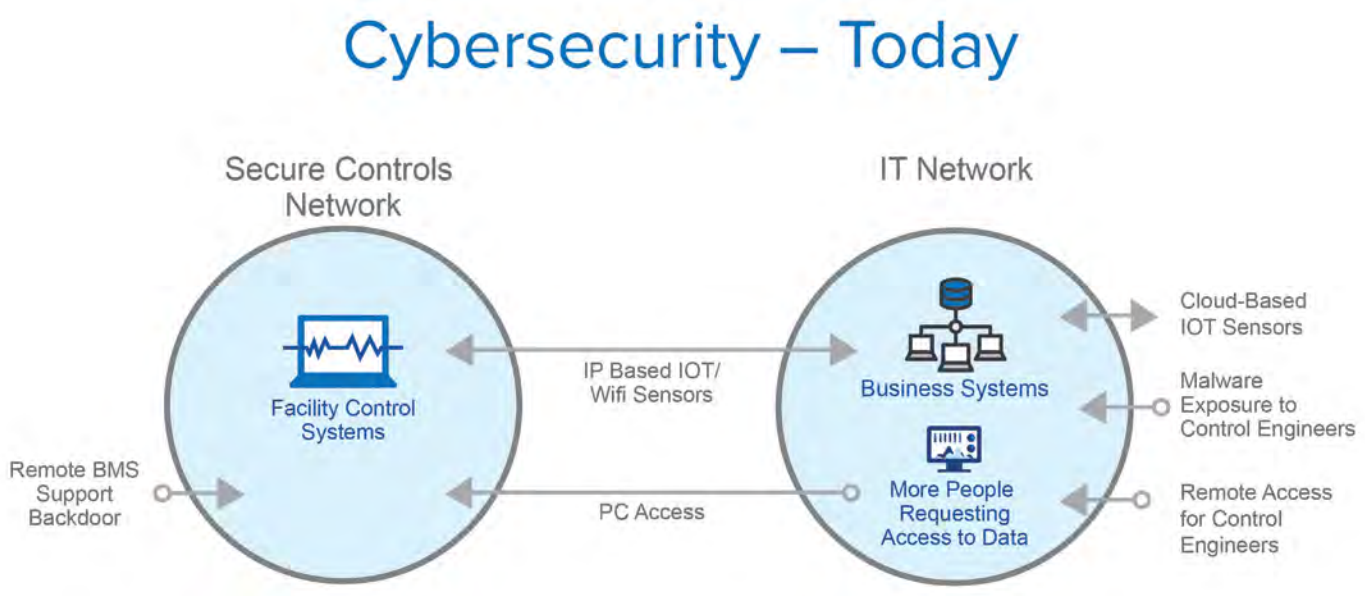
Ismail Sadiron / Shutterstock.com

5. HACKERS ARE BECOMING MORE SOPHISTICATED

Cybersecurity knowledge is evolving quickly. It's frighteningly easy for hackers to get access to many BAS. **Using Shodan.io, the first search engine for Internet-connected devices, a 5-minute search can produce log-in screens for multiple building management systems.**

And there are other tools and techniques — like Maltego and ZoomEye — that hackers can use to identify and compromise building control systems.

As organizations find and neutralize risks and vulnerabilities, hackers try newer methods of exploiting systems. The SANS Institute, one of the largest sources of cybersecurity training and certification, says that one of the newer areas of vulnerability being seen in 2018 involves data repositories / cloud-stored data. Software applications with vast online code repositories for collaboration and terabytes of mission-critical data stored in the cloud are increasingly common targets for attackers. Hackers search such infrastructures looking for passwords, crypto keys, access tokens, and sensitive data.



Many building automation systems ride on the enterprise IT network and allow multiple access points, leaving the control systems vulnerable to cyber attack.

REDUCING THE RISKS

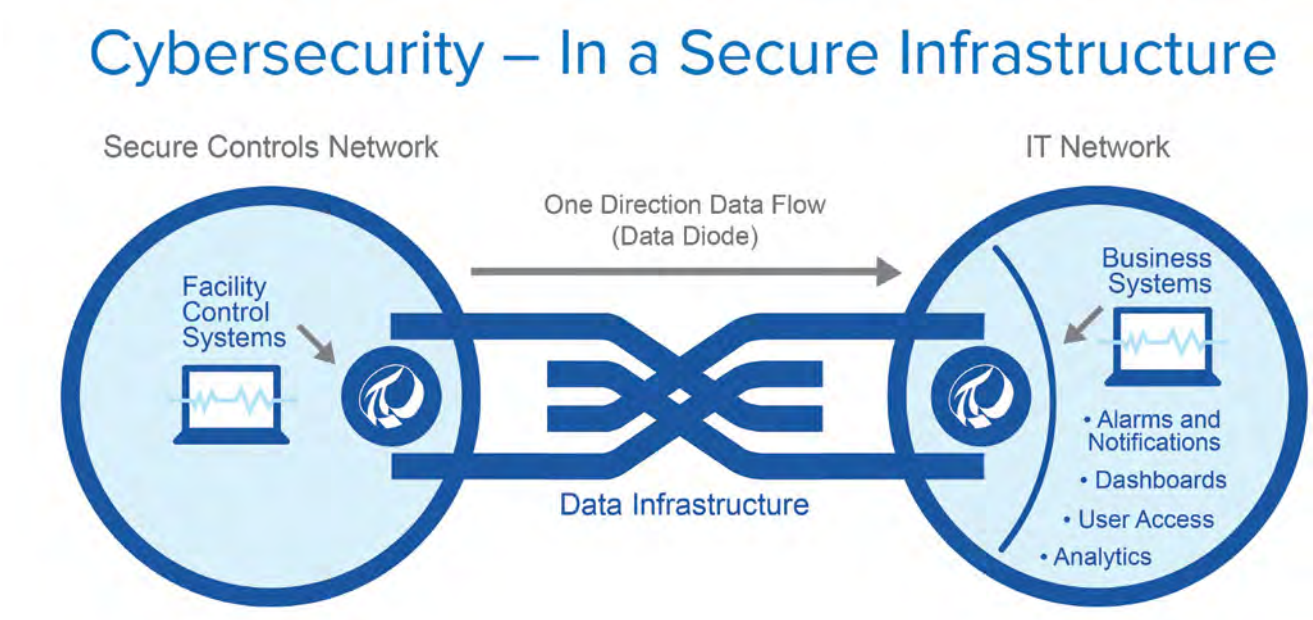
With so many areas of risk to building systems and data, what can be done by facility professionals to help reduce the risk? Here are four action items, and a list of questions that facility executives can ask of their team and their partners to help ensure secure systems.

LEARN FROM INDUSTRIAL CONTROL SYSTEM EXPERTS

While today's commercial and institutional buildings may lag behind industrial facilities in terms of cybersecurity, there are many parallels between a building management system and an industrial SCADA system, so there is much to be learned from industrial cybersecurity experts.

High-profile cyberattacks on critical but poorly protected industrial systems around the world have led to new awareness, better best practices, and good lessons that can be applied today to commercial and institutional facilities that want to make data accessible while protecting access to control functions.

OSIsoft, which started in the industrial space, is currently collaborating with the NIST National Cybersecurity Center of Excellence (NCCoE) and others on a project to improve the security of manufacturing industrial control systems. More recently, OSIsoft has partnered with NIST NCCoE to increase the development and adoption of cybersecurity technologies and business cases across industries.. They are working to accelerate the adoption of standards-based cybersecurity solutions that can be applied anywhere. OSIsoft's PI System has already been implemented to access and secure power-generation and energy-use data at MIT in Boston, NASA's Langley Research Facility, the Harvard Medical School, the National Institutes of Health, and the University of Maryland College Park campus.



A data infrastructure, the PI System segregates control system networks from data collection and distribution networks.

IMPROVE SITUATIONAL AWARENESS

OSIsoft previously partnered with the NCCoE in the development of the NIST Cybersecurity Practice Guide-Special Publication 1800-7, which helps utility companies measure and improve their situational awareness. Situational awareness allows managers of facility control systems — whether they are for power-generating systems like a cogen plant, water treatment facilities, or building systems like BAS — to monitor real-time data to find and fix problems, prevent issues, and optimize operations. Situational awareness is also essential to securing networks and reducing the risks associated with cybercrime because, for example, you won't know you have a breach if you don't monitor what's going on.

ANALYZE DATA ASSOCIATED WITH EVENTS

Data analytics takes situational awareness to the next level by contextualizing real-time data using "event" designations and notification functions.

An event can be anything with a start and end time — the startup and shutdown of an HVAC system, the time during which a room is occupied, or a campus-wide power outage, for example. Notifications are alerts that are generated when an event of interest is detected.

Using the PI System to enable data analytics is easy because the necessary functions are built in. These combine datapoints, calculate additional values, and implement or recommend additional actions so operators can save money, diagnose problems, and optimize operations. Event Frames capture the start time, end time, and duration of events, and as well as any other events or data happening simultaneously. The Notifications feature lets users configure rules that send email messages or call a web service when a specific event happens. All Notification actions — such as send times, acknowledgments, entry of comments, and escalations — are stored for later retrieval and examination. This enables a series of events to be captured and analyzed.

USE LAYERS OF SECURITY

Cybersecurity experts agree that the best security takes a layered approach. Just as the control systems of a nuclear power plant shouldn't run on a regular IT network, a BAS should not ride the IT network. That's one layer of protection that users of the PI System enjoy, because it segregates control system networks from data collection and distribution networks. This ensures that there is only one password-protected "door" for accessing facilities data. The PI System makes data accessible without exposing the BAS.

Other layers of security include making sure that every in-house user and vendor has a unique user name and that no one shares credentials, says facility cybersecurity expert Fred Gordy. It's also important to establish a periodic inventory of people granted access and devices connected to the system, as well as to make sure passwords are changed regularly.

Facility executives themselves can find out if their BAS has a public IP address and, if so, remove it and get the system behind a firewall, adds Gordy. If remote access is needed, choose one of the low-cost remote-access solutions that are available. These two steps alone hide your control system from search engines like Shodan, he says.

ASK MORE QUESTIONS

The following is a list of questions to consider:

- Have you thought about how data and control could be used to undermine your mission?
- How are you keeping up with what's happening with cybersecurity?
- What are the security parameters around your BAS?
- Do you use a third-party vendor for these systems and do they remotely connect?
- Do you combine operational data with outside data sources? If so, what associated risks are exposed?
- How are you getting your energy efficiency data?
- Can you identify when a cybersecurity event occurs? Have you identified any in the past six months?
- Can you act quickly if a cybersecurity event is detected? Who decides next steps?
- What data do you consider worth protecting? Have you done a data asset inventory?
- What are your vendors and partners doing to help you ensure your systems and data are protected?

The most important next step may be to ask questions of your team, and be sure they ask questions of their partners.

CONCLUSION

The growing availability and use of data are transforming the way that buildings are managed. Data is helping to make buildings more cost-effective to operate, to increase occupant comfort, to respond quickly to prevent system outages, and even to attract and retain the talent that the organization needs to grow. At the same time, facility executives must address the risks that come with the new generation of smart, Internet-connected devices.

The PI System can serve as the foundation of a cybersecure smart building. As a data infrastructure, it gives facility executives a secure means to standardize, integrate, and centralize data from disparate sources.

ABOUT OSISOFT

OSIsoft is dedicated to helping people transform their world through data. OSIsoft's PI System captures data from sensors, manufacturing equipment and other devices and turns it into rich, real-time insight to improve productivity, make critical decisions and develop new products. Over 1,000 leading utilities, 90 percent of the largest oil and gas companies and more than 65 percent of the Fortune 500 industrial companies rely on the PI System to get the most out of their businesses. Worldwide, the PI System manages over 2 billion data streams. To learn more, please visit www.osisoft.com.

Visit https://explore.osisoft.com/l/facilities to learn how our customers are using the PI System to improve their facilities, or visit http://explore.osisoft.com/l/osisoft-and-pi-system to learn more about OSIsoft and the PI System.

You can email us at smartbuildings@osisoft.com.

OSIsoft.

Corporate Headquarters:

1600 Alvarado Street
San Leandro, CA 94577, USA

Contact us at +1 510.297.5800