AWAIR

Why You Should Care about Data Security in Your Smart Buildings

It seems like every day there is breaking news about cyberattacks. As the digital age becomes increasingly interconnected, customers are relying on technology to run their buildings and make informed data-driven decisions. This is especially true when they're investing in indoor air quality (IAQ) monitoring devices.

These devices not only measure a variety of IAQ factors, but provide key insights into longitudinal trends. While this information is meaningful for health and safety decisions, it may not be data that a company wants shared with the general public. Additionally, since IAQ technology can easily integrate with other apps and tools, organizations need to be sure that proprietary data is secure across all building automation systems.

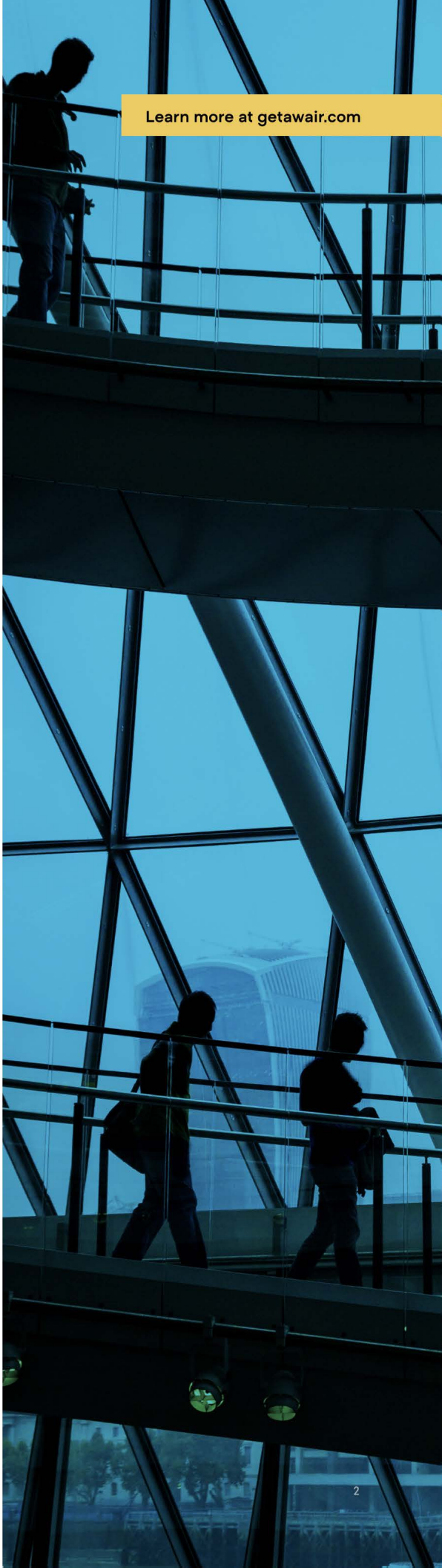
Real-World Examples of Cybersecurity and Smart Buildings

For facility managers and IT professionals, if you are considering beefing up the security of your company's smart buildings, now is the time to take action. There are many precautionary tales you can find around data breaches. And although no one ever plans to be the subject of a story like this, buildings with smart technology are susceptible. Hospitals, banks, retail stores, and technology companies are not immune to hackers looking for vulnerabilities within smart building systems (SMS). To avoid expensive and damaging consequences, brands need to rely on preventative data security practices.

To emphasize the importance of data security, we're sharing a few real-world examples. Within each situation, there are valuable lessons to learn from, especially as you implement tools for early detection and/or risk mitigation.

- A smart thermometer in a **casino lobby fish tank** gave hackers access to a high-roller database in 2018. Someone got into the fish tank, which had sensors connected to a PC, and used it to move around into other areas of the network. While the casino's name was not disclosed, the report showed that 10 GB of data was sent to a device.

- At a **German office building**, there was unauthorized access of a building automation system (BAS). The owners were locked out of the system and three-quarters of several hundred devices were non-operational from office lighting to motion detectors. BAS devices were not restored until a few weeks after the hack. Unfortunately, cyberattacks on



buildings have the power to wreak havoc on occupant safety and comfort.

- A **commercial high-rise between 40-50 floors**, two of which were government offices, was targeted by a hacker. Through an exposed wireless access point, the parking system printer was penetrated. The printed message said there was a bomb in the building. Needless to say, this wasn't a great look for the office building or the brand.

How To Take a Proactive Approach to Protecting Your Data

There are several data security practices that organizations should look for in their indoor air quality devices. The first is focused on **SOC 2 Type 2**, which is Service Organization Control. This internal controls report details how the technology safeguards customer data and how the controls are operating. Your IAQ partner should be able to address questions from your IT or Security teams on SOC 2 Type 2 Compliance.

To test vulnerabilities in the IAQ device system, a security penetration test or "**PenTesting**" is also essential. An independent third-party company should work with your IAQ partner to ethically hack their system. Ultimately, this procedure will test the robustness of their security. You may want to ask if the IAQ company has security risk management software so they are continually scanning for threats. An example of an identified threat would be Log4j, which was a security bug revealed last year by Apache Software Foundation. Having a plan in place for security threats can make the difference between secure and insecure data. Trust us – there is a **big** difference with these two realities.

Leveraging identity management platforms, such as Okta, OneLogin, or Ping Identity, can also help to streamline your IAQ security. With a **Single Sign-On Service (SSO)**, your administrator can invite and grant access to your IAQ application and analytics dashboard using a method central to your organization. You can simplify the user experience and reduce the risk of your users having to maintain multiple logins.

"Given **that companies use 16 SaaS applications on average**, it is clear why SSO is a common feature request among enterprise and mid-market companies." Adding extra layers of security should not be a "nice-to-have" quality in your IAQ partner. It's a must. IoT-enabled equipment is vulnerable to hackers, but you can have a strategy to protect smart buildings and keep building occupants safe and comfortable.

Selecting an IAQ Vendor for Your Company or Organization

As you get underway with researching IAQ vendors, you will want to involve your Facilities Management (FM) and IT and/or Security teams. We've compiled a list of helpful questions to ask as you begin your search. What's important is that both teams think about data security. One team should not make data security vetting the other team's job. All sides should work together so key details are not missed.

10 Questions Your IT Team Should Ask

- How and where is data stored?
- How do you manage remote access to data?
- How often is data backed up?
- How is user-access managed?
- Do you have SOC 2 Type 2 security certification?
- Can you provide the results of your most recent external security audit?
- Do you conduct regular "white-hat" penetration testing of the platform?
- Does your solution have hardware or software "backdoors?"
- Does your solution have any hard coded or unchangeable user-accounts and credentials?
- Does your solution have any removable key components or modules?

10 Questions Your FM Team Should Ask

- What does your IAQ device measure?
- How will this device keep building occupants safe?
- How does this device alert us to potential issues?
- Is the IAQ sensor energy efficient?
- How quickly can I get the device up and running?
- Can I manage the IAQ data of multiple campuses?
- Does the device meet specific compliance (i.e., WELL)?
- How often will I need to replace the devices?
- How will the monitor inform changes needed?
- Where should I place the monitors to start?

Recap: Data Security Practices in Smart Buildings

Data security is more than having the right tools in place, you need to have the right partners to help you along the journey. As you implement devices and technology to measure your company's indoor air quality, make sure your vendor is ready to answer questions from your IT/Security and Facilities Management teams.

Instead of being fearful of potential hacks, you can ensure that your building automation systems are ready to combat threats. During your exploratory conversations with IAQ vendors, we suggest looking for partners who understand data breach implications from all standpoints, including financial, reputational, and safety.

If you have any questions along the way, **please reach out to our Awair experts**. We'd be happy to get you started with securing your company's IAQ data. If you want to learn more about the security protocols we take related to SOC 2 Type 2, PenTesting, or SSO, we can dive into greater detail and share some best practices as well.

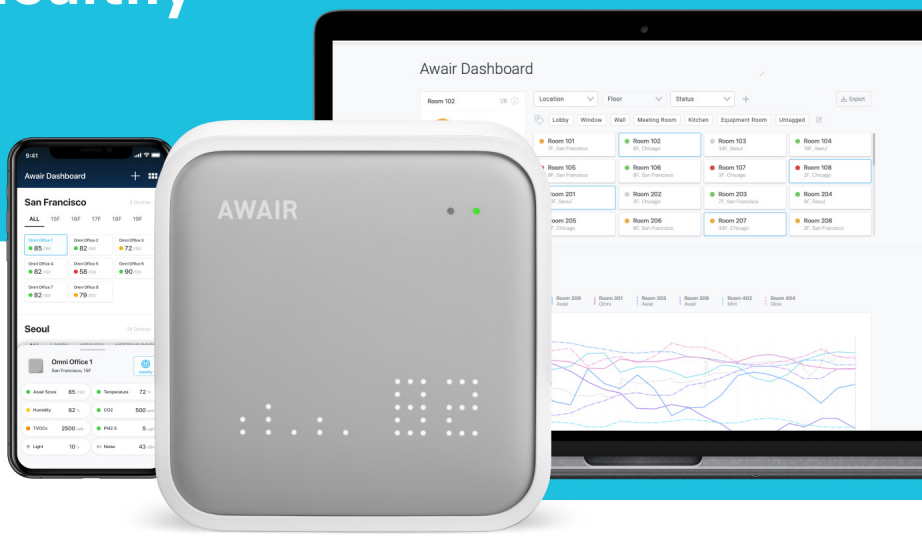
How is your building's air right now?

Awair Omni features enterprise-grade sensors that track temperature, humidity, CO_2, chemicals (TVOCs), fine dust (PM2.5), light, and noise. A software dashboard and/or API provide air data as well as actionable insights so you can take control of the air in your environment no matter where you are.

Omni is already used by leading organizations like WeWork, AirBnB, Harvard, Stanford University, and Google to keep their facilities optimized for employee and tenant health.

Let's keep the air healthy

Learn More



AWAIR