# How to combat vulnerabilities in home automation

When it comes to cyber security, the industry has been vocal about its commitment to best practices and education as it relates to video surveillance and access control solutions. Integrators have become increasingly proactive to ensure they are delivering the best solutions possible, while simultaneously providing the highest level of security. While video systems have traditionally garnered much of the focus as it relates to cyber security, there's a new kid on the block who is gaining much attention from hackers with malicious intent: home automation.

Home automation has become a convenient normality in residences across the world. While turning lights off and changing the temperature with the sound of one's voice is a perk, smart homes are capable of so much more. Automation improves daily lifestyle, but also provides a security solution accessible from anywhere. Users can keep an eye on their homes from their cell phones. They are able to check to make sure the kids get home safe or confirm their package is delivered. It is presented as a convenience and much of its implementation has revolved around that. Where there is convenience for end users, there is also convenience for hackers. By using devices that connect to the internet, there are inherent security risks. It is the job of the security system integrator to be sure their clients are protected.

## Checking the boxes

The first thing integrators should do is make sure the system is encrypted. This probably seems obvious, but is the first line of defense against potential threats. It is one of the best methods of safeguarding privacy. This is especially important when protecting people's homes. We live in a world of constant connectivity – whether through phone calls, emails, online purchases, or social media. Actions that seem innocent, such as setting up a recurring delivery for pet food, can actually pose some big threats. Hackers are becoming increasingly interested in targeting homes because unlike major corporations, most system users are not security professionals. IP-based systems in homes have not traditionally had the same level of security as those in the corporate world. Home owners believe once a system is set up, they are good to go. With the right integrator, only after security measures have been implemented, this is the case. Without encryption in place hackers can easily intercept online logins, banking information, and can discover schedule patterns for when doors are locked and unlocked such as when people are home. Gone are the days when passwords were enough to secure your life from intruders. Integrators need to encrypt everything to be sure cyber integrity is upheld.

The second thing integrators should do is set up multifactor authentication to validate the connection and be sure the data is only accessible by the homeowner. This protects data while simultaneously assuring that the homeowner is indeed the homeowner. Hackers can guess passwords but the odds of them breaching multiple levels of authentication are slim. The more factors set in place create the reduced risk of an intruder gaining access to a private system. It is best to combat attacks before they happen, rather than wait for a system to be compromised.

As the saying goes, it is not a matter of “if” a user will fall victim to a cyber-attack, but rather “when.” Multiple layers of security are a good practice to deter potential hackers.

Third, integrators need to be sure the system stays updated. If the system is not regularly updated with patches, then over time hackers will find new ways to infiltrate it. Just as humans need a new flu shot every year to protect against changing virus strains, security systems require the same level of routine maintenance. The industry is constantly evolving for the better. However, as fast as new technologies evolve, so do new hacking methods.

**Why home systems now?**

Hackers are always looking for soft targets. As big corporations and smaller businesses up their cyber security game, what better target than an unsuspecting home owner without an IT team at their disposal? Homes equipped with automation are being targeted because they have multiple devices that connect to the internet and, as we know, an internet connection means cyber vulnerabilities. The more devices a user has, the more vulnerable they are to cyber-attacks.

Wireless doorbells, keyless entry, digital thermostats, and lighting systems are a few of the ways hackers are gaining access to homes today. Because the systems in a home automation setting are controllable via Bluetooth or internet connection, it opens the door for hackers to use a seemingly innocent device, such as a wireless doorbell, as a point of entry. This allows them to then gain access into something of higher importance, such as a computer. From there, hackers can gain access to a users’ most private information, including banking information, passwords, or lock/unlock schedules.

Once a hacker gains entrance to a home system, users fall vulnerable to cyber physical attacks. Cyber physical attacks occur when hackers are able to intrude over the wire/internet and enable an action such as disabling security systems then physically entering homes to steal or hack information directly rather than remotely. Home automation opens the door to new threats both literally and figuratively. Establishing baseline requirements when selecting vendors is the most necessary and responsible measure an integrator takes.

**How do you choose a vendor?**

Integrators can utilize best practice solutions, but one of the most important aspects of their job is the vendor selection process. By making sure the product has built-in security protocols, it alleviates the need to take additional steps and saves both the integrator and user time and money in the long run. Home owners are bringing experts in to simplify the process as much as possible; what simpler way than choosing products with out-of-the-box capabilities?

Home owners who choose to implement home automation solutions do so with the understanding that it is easy, streamlined and risk free. Most people are not cyber security experts and in turn expect whoever they’re contracting with to provide top-of-the-line service and recommendations. The challenge for integrators in this scenario is not in implementing best practices, but rather in choosing cameras and solutions that will ensure the maintenance of its cyber security. As in any market, manufacturers compete to provide the latest and greatest solutions, but often the race to be first leads to long-term issues. There is great pressure to make cutting edge solutions available. This idealized manufacturing timeline typically results in products that are not completely vetted. While some companies go about deployment in a mature way, by designing cameras with cyber security in mind from initial development, others position cyber as a second thought compared to functionality. In turn, system integrators must do their research to select cameras that include both functionality and security. Also they must not be afraid to ask the supplier questions such as: Have they deployed a secure development lifecycle policy? Is communication encrypted? Why is your camera better than someone else's? Integrators are advocates for their customers and should recognize that the latest solutions are not always the greatest.

Integrators should always think ahead and anticipate what might be a vulnerability in any system. While a low-cost device, such as a motion sensor outside the home, will save the user money, it can also enable some activity that could ultimately raise a risk for the homeowner. In some instances, this can force both the integrator and the user to compromise. If you cannot trust the connectivity of a particular device that is costly, you may opt to use a less-modern solution, such as wires, that uses technology that is not accessible from the internet. It is important to not just look for the cheapest solution, but to implement the one that will not raise the risk level for end users. Functionality, cost and security should be the three determining factors when creating a solution.

## The future

Cyber-attacks are expected to increase, especially as home automation technology continues to evolve and becomes more readily available at a reasonable price. Hackers do not care about someone's business, livelihood, or peace of mind. It's critical that security system integrators also ensure that home automation systems can exist in a way that will not pose a cyber security threat. Homes should be a safe haven, and it is the integrators job to keep it that way.