News

IoT & Smart Technology opens up new doors that require protection

Technology is a part of our day-to-day lives, with smart devices in our homes and the ability to perform tasks at our fingertips now a reality. This transformation is significantly impacting the physical security industry. No longer are the cloud and the Internet of Things (IoT) distant concepts full of intrigue and promise. We're seeing these elements increasingly incorporated into security solutions today, allowing organizations to experience countless benefits when it comes to both safety and business operations.

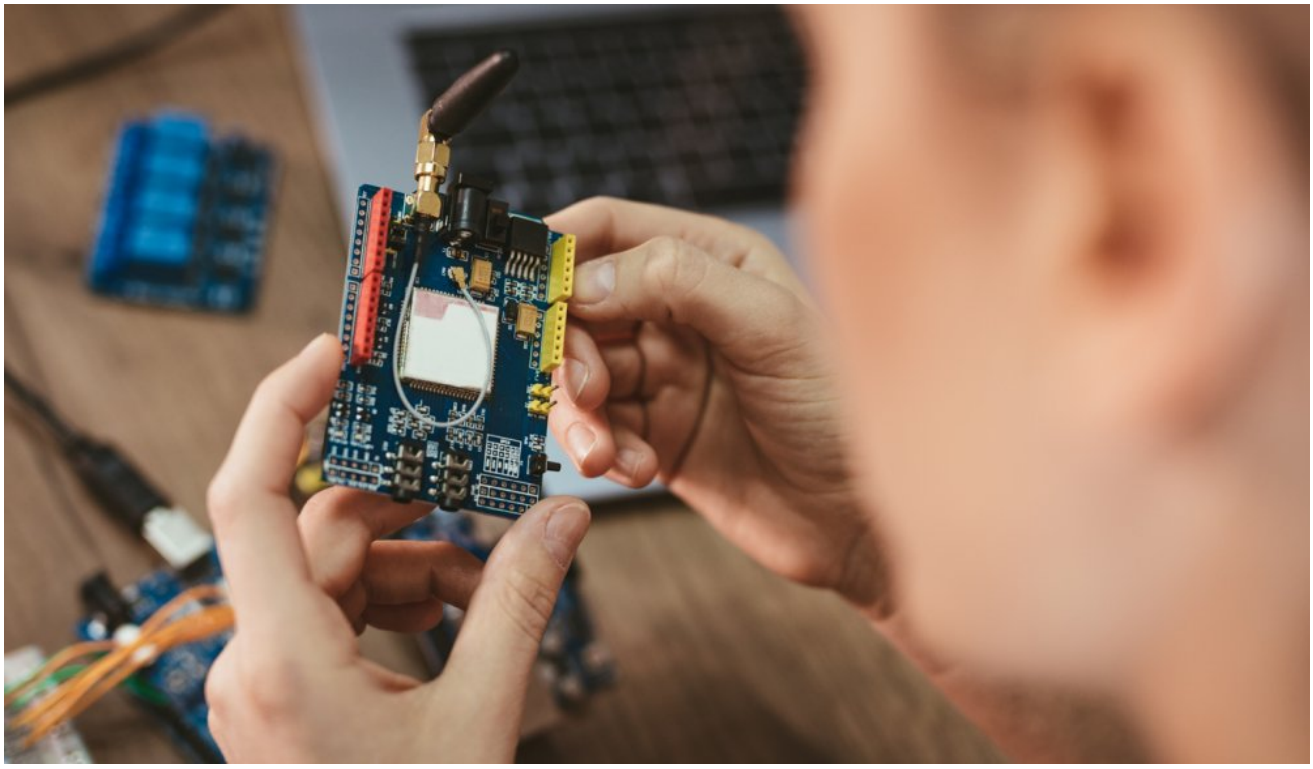
Now that we're past wondering what these technologies will bring to the industry, we can start to look at what the future holds. It seems the positive possibilities for smart technology are endless, and the general public certainly appears to be on board. For instance,

Cambridge-based tech company, Arm, commissioned research firm NorthStar to survey 2,000 global consumers. It wanted to discover consumer insight on 2018 technology trends and their expectations for 2019. It also asked its technology experts and futurists what they think will happen within IoT technology over the next year and beyond. The convenience of smart technology is the main reason to "love" (26 percent) or "like" (37 percent) the technology.

With that in mind, **Ross Wilks, Head of Marketing Communications** at Vanderbilt, gives insights on the company's views and outlook on the IoT world and smart technology as a whole.

With the current popularity of IoT devices, what should consumers keep in mind when it comes to the security of these technologies?

Wilks: Absolutely. The convenience of IoT technology is undoubtedly popular with consumers. However, as a natural parallel consequence, the security industry is seeing significant demand for the incorporation of cybersecurity practices into physical security systems. A higher level of cybersecurity awareness has led the industry to realize that one of the most critical areas that this need for protection comes from is within the communication between devices. So, while the cloud and IoT have opened many doors for interconnectivity, inherent vulnerabilities can lurk beyond each entrance without proper security best practices. It is therefore essential that these valuable, yet susceptible paths of communication be safeguarded at all times. Even if a physical security solution is doing its job, such as an intrusion system providing an alert for an incident, an organization is still not comprehensively secure when the method of communication for that alert is exposed.

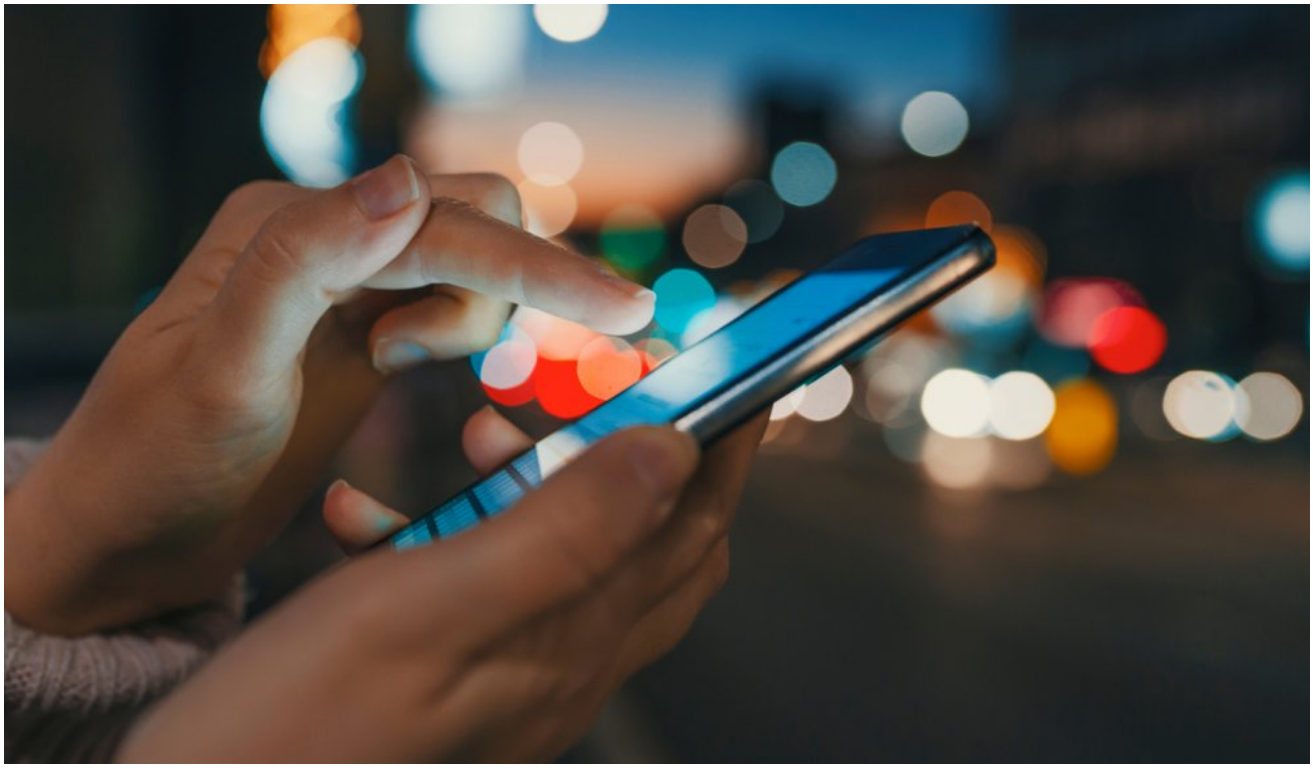


And of course, a frequent target for cyberattacks is the access to data. How can information be protected against?

Wilks: That’s right, the transmission of data has become such a vital part of the efficiency and effectiveness of today's security solutions, but unfortunately, it has also turned into a common target. Communications protocols such as Vanderbilt’s FlexC can help establish a fortified method of transmission, allowing physical security systems to safely do their job. FlexC is a multipath, multi-redundant, highly encrypted communications protocol that allows secure monitoring and control of IP communication paths. Built from the ground-up and solely with cybersecurity in mind, FlexC is a bespoke design that takes into consideration multiple types of attacks for defensive purposes, facilitating comprehensive protection and an exceptionally secure cloud network. One of the apparent drawbacks of IoT devices is that they are based on the concept that everything is accessible. And when it comes to security, it can only take the weakest domino in your defensive lines to fall before your security is comprised. Vanderbilt tackles this IoT issue through a slightly different approach. Instead of making everything accessible, Vanderbilt try to securely allow access to additional devices through a gatekeeper system. For instance, communication with an SPC Wireless PIR sensor is facilitated directly through the main SPC system itself.

So, in essence, the SPC system is acting as a gatekeeper for all peripheral products it operates with?

Wilks: Exactly. The SPC system acts as a gatekeeper to protect all individual devices working in conjunction with the SPC panel. This also expands out to other downstream connections, such as third-party integrations working on different buses. This is because SPC has built-in protection mechanisms whereby if the system is attacked, it will go into protection mode. The system will remain operational, and it will still be able to communicate out, but it will start to shut down elements of itself to protect the system from the attack. While no system is invincible, SPC has been designed so that should an attack penetrate, the system has multiple communication paths available as a backup. Therefore, if one server is taken down, the system can immediately switch to a backup server and then change communication paths to bypass the attack and ensure messages still operate successfully. This makes the SPC system a secure gatekeeper to facilitate communication between Vanderbilt's IoT devices such as the SPC Wireless range. This provides the benefits of IoT without exposing the devices to all of the risks associated with IoT, in turn, maximizing the functionality of the product. Moreover, the SPC system has recently been accredited to the NF A2P Cyber-RTC cybersecurity standard from the CNPP. The SPC intrusion system was tested by CNPP to ensure that it meets the latest needs for cybersecurity. This is part of Vanderbilt's continuous endeavor and commitment to work with approval bodies to ensure both the best-in-class security and the confidence that your security system is secure.



How important is it to be certified to the NF A2P Cyber-RTC standard?

Wilks: By certifying the SPC intrusion ranges on the latest CNPP NFA2P at Cyber Type 2 and 3 repositories, Vanderbilt can ensure it is providing all its customers with high-level security for all remote monitoring transmissions, as well as for cloud applications such as SPC Connect. The market is flush with cybersecurity standards, but the NF cybersecurity standard from CNPP is the first developed explicitly for intrusion alarm systems making it an excellent way to benchmark and improve SPC intrusion systems. And as smart technology continues to rise to the front of security solutions, growth of the SPC Connect cloud application continues to boon. Right now, the numbers for SPC Connect are meteoric. In just over two years, the product has won all sorts of awards for alarms and innovation. SPC Connect's interconnectivity is making a clear difference in how installers conduct their business, with the whole ecosystem that the app's features have now built becoming a vital extension of their daily business. A quick look at the numbers shows that since mid-2016, the solution has racked up over 1,000 installer customers. Connect receives over 32,000 login requests every day. An average of 24,000 push notifications and 12,000 emails are sent from the solution per day, with roughly 85,000 commands being sent from Connect to SPC panels each day through the bespoke communications protocol, FlexC.

So, all in all, SPC is proving to be right at home in the new world of IoT and smart technologies?

Wilks: Yes, SPC is proving to be an adaptable intrusion system on this new front. Making further inroads on the smart technology era, SPC also integrates with several third-party smart technology products like Homey, a smart home platform developed by the Dutch company Athom. As the SPC security system operates stand-alone, none of the certifications or assurances are compromised. At the same time, all sensors and data available in the system are available in Homey too, ready to be used in a smart home environment. Another such smart technology integration is with Dutch company Triplence Technologies' Aperium box. This has been established through Vanderbilt's aforementioned FlexC. When integrated with Vanderbilt's SPC intrusion panel, the Aperium box allows for combining intrusion alarm events with VCA verification and combining non-alarm events like Access Denied, Door Forced, and System Armed/Disarmed. Along with a series of snapshot images, this makes the job of the CMS operator more comfortable and increases the standard of security for end-users. Another positive benefit from this integration is that through the Aperium box, SPC can now be combined with a more

significant number of IP cameras of various brands, as well as other major brands of Network Video Recorders.

What do you think is the core reason behind this rise and advancement of IoT and smart technologies within the security industry?

Wilks: I think it all simply boils down to convenience. The internet revolutionized the security industry, and today, technology continues to evolve at a speed and depth that is changing the way people protect their premises. Smart technology simply deals with the need for convenience that this evolution has developed. It deals with things that are at the heart of every customer's pain points – time and money. Solutions like SPC Connect allow for the elimination of once tricky tasks that are now capable of instant execution through the quick click of a button on mobile or desktop devices. As summarized by a Vanderbilt customer recently, Dave Arys, the General Manager at Waasland Security, with SPC, "we now have a product that not only meets the end user's requirements but also the requirements of the installer." I think that sums it up quite nicely.