Why the Internet of Things Changes Physical Security
Please attribute to Per Björkdahl, ONVIF Steering Committee Chair

A search for the Internet of Things generates millions of hits on Google on any given day. Searches for Barack Obama and the World Cup generate much fewer hits, to give some perspective. The Internet of Things (IoT) is an idea that many people from across the world are talking about.

There is healthy debate on what constitutes an Internet of Things. Discussions about IoT often center on what IoT might mean to future technologies, product development and sales, without really defining it. Others argue that an Internet of things already exists, made up by the integrations of mobile, network and web-based applications, with Web 3.0 promising to deliver an even more personalized user experience. Some technologists believe that the term IoT only refers to the connection of objects to other objects, and have coined the term 'Internet of Everything' instead, which consists of the 'smart networks' needed to connect all of these objects.

There are also serious security concerns about the information exchanged when connecting all of these things together and creating new access points that leave the safety of a well-secured and finite network. Early IoT devices are already facing criticism for their vulnerabilities and their potential for poor security practices, covert data collection, loss of control of devices and invasions of privacy. Several well-respected figures, including Stephen Hawking, Bill Gates and Elon Musk, have expressed concern over the blending of IoT with artificial intelligence. They say there are real dangers in having machines make decisions and control objects.

The physical security community's discussion of IoT is somewhat different from those of other industries. Our business is securing things, people and information and we seek to make assets safe using a combination of physical barriers and technological tools. Our approach to IoT, therefore, naturally requires more caution and nuance than most. Those of us in the industry know that information is not only power, but that it can also be detrimental to physical security when it falls into the wrong hands.

The physical industry must exercise caution in developing products for IoT and capabilities. More data sharing inevitably means that a security breach on one device or system could result in vast amounts of data from many systems and devices being compromised. In fact, HP recently reported that up to 70 percent of commonly used IoT devices are vulnerable to cyber attacks. Another point for the industry to consider is the likelihood of new laws being developed to protect the end user's privacy, specifications to which the industry must adhere.

The integrity of the security we provide as an industry should not be compromised for IoT. Businesses, governments and people rely on us to protect

what is important and we must continue to maintain the high standards that currently exist in our industry today. That is not to say that the physical security industry should ignore IoT, but rather should be thoughtful and deliberate in its approach to IoT, as we develop new products, software and systems.

It is of particular interest that many within our industry and in the technology industry at large contend that standards are and will be the lynch pin to hold together and make IoT a reality. It is predicted that there will be a global IoT standard in place as early as 2016. The world's largest technology-based professional association, IEEE (the Institute of Electrical and Electronics Engineers), is already at work developing IoT standards for several technology-based industries.

Several alliances have also formed to work on automation and communication protocols to prepare for an increase in (machine-to-machine) communications and the broader IoT. These alliances, such as Zigbee, the THREADGroup, ZWave and HomeKit, include physical security manufacturers and organizations in their memberships. Some alliances have already developed certification specifications, some of which include video surveillance, intrusion and access control.

Standards will be fundamental to the development of IoT technology in the physical security industry, as many have predicted. ONVIF's interoperability standards were originally created to take usability to a higher level by allowing end users to pick and choose technology from different brands without sacrificing functionality between these devices. Similarly, IoT will require manufacturers and developers to work together in establishing baseline standards and specifications that will further allow physical security systems to not only work with other physical security devices, but also with other kinds of devices beyond the confines of our industry.

Though many questions remain, it is clear that the Internet of Things is already developing and growing in the broader technology market, as customers purchase more and more connected products and are predicted to buy even more in the coming year. Verizon, in its 2015 State of the Market IoT report, predicts that 10 years from now, organizations that use IoT heavily will likely be up to 10 percent more profitable, with data showing 204 percent growth in the number of IoT connections in the manufacturing sector. The Internet of Things cannot be ignored, despite its mix of potential boons and possible weaknesses. It has moved from a conceptual state to a budding reality, with some calling IoT the next phase of the industrial revolution. IoT will become a reality in the physical security industry, of this we can be assured, whether the industry is prepared or not.

Given the inevitability of the Internet of Things in the physical security market, the question to be asked is not if IoT will affect our market, but how best to prepare

for and approach IoT. The challenge, of course, will be to provide increased operability and ease of use for end users without losing the integrity of the security that we offer as an industry. We must determine how to best continue our job of protecting valuable assets while providing end users with the functionality, ease of use and interoperability they expect, balancing IoT's strengths with its weaknesses in our development of products and standards.