Published on *The National Law Review* https://natlawreview.com

The Internet of Things and the Inevitable Collision with Product Liability PART 5: Security and the Industrial Internet Consortium

Article By:

H. Michael O'Brien

The rapid emergence of the Internet of Things (IoT) led to the establishment of the Industrial Internet Consortium (IIC) in the spring of 2014 by five primary stakeholders: AT&T, Cisco, General Electric, IBM and Intel. IIC now claims a membership of 211 in more than 26 countries. Each of the five founding members, like many other companies, is undergoing significant transformations within their core business platforms to take advantage of the immense growth opportunities with IoT.

On November 3, 2015, the IIC held its initial Industrial Internet Security Forum at IBM's New York City headquarters. Not surprisingly, security, security and more security was the *theme du jour*.

Part of IIC's mission statement is "To bring together the organizations and technologies necessary to accelerate the growth of the Industrial Internet by identifying, assembling and promoting best practices." Its goals are to:

- Drive innovation through the creation of new industry-use cases and test beds for real-world applications
- Define and develop the reference architecture and frameworks necessary for interoperability
- Influence the global development standards process for Internet and industrial systems
- Facilitate open forums to share and exchange real-world ideas, practices, lessons and insights
- Build confidence around new and innovative approaches to security.

Guest speakers at the program were members of the IIC and security experts. Key takeaway points from this meeting include the convergence and friction between information technology (IT) and operational technology (OT); the inevitable identification of payloads for IoT cyberattacks; interoperability issues and defense of legacy technologies; and perimeter defense and partition of systems to improve security. All of these terms and concepts were addressed by speakers and panelists to define IoT security within the Industrial Internet.

Opening remarks by Lynne Canavan, IIC's Vice President of Program Management, emphasized IIC's mission statement and the charter of the Security Working Group to "define a security and privacy framework to be applied to technology adopted by the IIC." This "will establish best practices to be used to identify security gaps in existing technologies."

Key Drivers

Brian Dalgetty of IBM IoT, Industry Solutions, identified some of the key driving and disruptive forces of IoT, which include improving operations and lowering costs, creating new business models and products, and driving engagement and customer services. Among the challenges identified were (1) the unprecedented data volumes, (2) fundamental shifts in business models, (3) incompatible standards, (4) entirely new security threats and (5) the new privacy landscape.

While big data is one of the driving forces behind the IoT, Dalgetty observed that 60 percent of data collected loses its value within seconds. Part of IBM's strategy is to partner with companies that provide services for the IoT, and not necessarily to make new things. IBM wants to capture data and use it to transform businesses. To that end, it is developing horizontal platforms with partners. Collecting and capturing the data, however, is not the end game. The application of the data is the new game.

One innovative IoT application identified was Daimler's Car2Go, which is a new concept for renting vehicles. Among the new features is providing insurance as well as a menu of options to have interconnectivity services with the vehicle. Airbus was another example of a company that is

optimizing operations and performance with real-time monitoring of critical components in their aircraft engines. Among the benefits of optimizing operations is to increase the resale value of aircraft by as much as 20–25 percent due to the employment of advanced maintenance features.

Health Care and the IoT

Beth Hoenicke, Senior Integrated Computer Solutions strategist with Johns Hopkins University, discussed many of the advances IoT will make in the health care industry. She described a digestible pill that when swallowed by a patient would allow a medical service provider thousands of miles away to conduct a diagnostic analysis. She referenced a McKinsey & Company forecast that 40 percent of the Industrial IoT will be in the health care industry. However, there will be a lot of data “exhaust” (pollution) from all the information generated. In addition, the continuing use of legacy technology with IoT will present challenges.

While harmonization of standards is a desirable goal, Hoenicke noted that “one size fits all” is not achievable, so there will be challenges among industrial sectors, as well as between the advanced nations at the forefront of the development of IoT and the less-developed nations to work out standards that will help with interoperability of different platform applications of products.

Encryption

Steve Hanna of Infineon Technologies discussed the use of advanced chips with encryption to help secure IoT products. He noted that while the need for software patches will be inevitable as there is widespread agreement that there is no software code written that does not contain vulnerabilities, the use of encrypted software patches is viewed as a means to prevent reverse engineering of patches and can help prevent counterfeiting by competitors. However, security challenges exist in network systems, software and the cloud.

Infrastructure: OT versus IT

Jesus Molina, Security Consultant, Fujitsu, and co-chair of the Security Working Group for the IIC, discussed the challenges faced by an aging legacy infrastructure. Industrial systems with cyber-physical components were created with security assumptions that are no longer valid. He noted the distinctions between IT and OT and that in the past there was a separation between the two, but they are merging and in a short period of time may be indistinguishable.

With OT, the first priority is safety to prevent injury or death, preserve the public welfare and avoid an environmental catastrophe. The second priority is reliability of the operation of the machinery and infrastructure. Among the challenges is that OT generally has a slower path to an upgrade whereas IT can be upgraded routinely on an almost daily basis. Old technology deployments being married with new technology was also identified as security vulnerability. Older technology deployments will not go away due to the significant capital investment required to develop the new technology deployments. Molina also emphasized that with so many IoT-connected devices and their vulnerabilities to hacking, it is only a matter of time before hackers identify “payloads” that will drive the monetization of the cyberattacks. This pattern is similar to what occurred with the development of PCs and servers. Hackers were initially able to gain access to them, but it took time before they realized the opportunities to secure confidential data and financial information and thereby monetize their criminal activities.

Convergence

The program concluded with a panel discussion moderated by Francis Cianfrocca of Bayshore Networks. The panelists included (1) Tim McKnight, Global Chief Information Security Officer with GE, (2) Demitrios Pendarakis, IBM Watson Group, (3) Brian Witten, Symantec, and (4) Mike Firstenberg, Waterfall Security. The panel discussed the convergence of IT and OT as a crucial challenge faced by the Industrial Internet of Things. OT deals with the maintenance and operations of the machines that are required to run 24/7. The challenge for IT is to monitor and constantly ensure the security of the software program operating the new IoT industrial applications. The two tech teams do not always see eye-to-eye and at times can feel challenged that each is working at cross purposes to the other's goals. However, without the cooperation of the two, the Industrial Internet of Things will remain vulnerable. Nation state hacking and organized criminal hacking were also identified and discussed as being present threats that will remain threats for the foreseeable future.

The development and deployment of IoT across so many industry sectors is beginning to reveal the patterns of similarities in security concerns as well as the unique challenges that each technology sector will be required to confront as product and service platforms emerge. Meanwhile, the steps being taken by the IIC to establish a framework of open cooperation and sharing of ideas and experiences holds some promise that the inevitable collision of product liability and cyber security issues will be mitigated to some extent. Ideally, as threats are identified, new solutions will be developed and shared across industry sectors.

National Law Review, Volume V, Number 329