July 20, 2017

Cybersecurity Risk to Industrial Internet of Things: Not Just IT Problem

The Industrial Internet of Things (IIoT) hits center stage again for cybersecurity awareness and protection efforts with many associated legal issues to consider.

Another Notice of the Escalating Risks

Earlier this week, InfraGard[1] distributed a broadcast message titled "Anticipatory Awareness Message: Cyber Security for Smart Manufacturing."[2]

> This notification is based on anticipatory analysis of emerging technology vulnerabilities and historical cyber intrusion activities. It is intended for companies and organizations that are using smart manufacturing technologies in their production or research efforts.
>
> **The FBI and the National Center for Manufacturing Sciences (NCMS) assess that smart manufacturing technologies and equipment likely are vulnerable to malicious compromise by a variety of cyber intrusion techniques. Such intrusions have the potential to target proprietary design, business, and other manufacturing process information.** We have medium confidence in our assessment based on the increasing connectivity of web-based process automation, data analytics, and connected industrial control systems (ICS) involved in modern manufacturing.
>
> Smart manufacturing is often referred to as Industry 4.0 or the Industrial Internet of Things (IIoT) and broadly refers to Web-enabled or networked cyber-physical manufacturing technologies. The integration of network connectivity into manufacturing technologies significantly increases the attack surface for malicious cyber actors, and creates a number of points for penetration or pivoting into other critical network segments.
>
> Production equipment or other advanced technologies associated with smart manufacturing may not necessarily be designed with cyber security in mind. Further, integration of legacy manufacturing equipment into a networked environment may create additional cyber vulnerabilities. As such, security of information technologies (IT) and operational technologies (OT) should be considered in parallel when integrated in a manufacturing setting.
>
> Given the sensitive, proprietary design and process information contained in design and manufacturing process data files, the FBI and NCMS recommend equipment operators and system administrators apply rigorous cyber security practices when incorporating the technologies into their production facilities or hosting the technologies on their networks. Information that transits a manufacturing network should be considered as sensitive as other business-critical information, and should be protected as such.

This assessment follows a highly publicized report in June regarding similar and specific risks involving the electric grid, related to malicious software called "CRASHOVERRIDE."[3]

What Can In-House Counsel Do?

Companies with strong compliance programs are well-suited for addressing the ever-increasing risks associated with the IIoT. While the IIoT permits industrial, manufacturing and energy companies to realize significant benefits in efficiency and capability, as the two material warnings illustrate, the IIoT also creates new risks that need to be considered. The following assessments may help in defining the risk to your company and identifying appropriate mitigation strategies:

- In light of the warnings, and a company's current and projected IIoT-related structure, are proper resources in place to ensure regulatory compliance? Where cybersecurity plans are required by regulation (or have been voluntarily adopted), do they adequately encompass the company's IIoT-related structure?
- Do existing contractual and other relationships between the company and partners, vendors and customers, which may involve the use and operation of shared IIoT elements, adequately allocate ownership, responsibility and risk? In the event of a cybersecurity event such as warned against in the InfraGard report, can the company respond in an efficient manner consistent with existing contractual and business relationships, many of which may have been established and documented long before adoption of IIoT technology?
- Do existing insurance arrangements adequately reflect the liabilities which could result from the types of events reflected in the InfraGard and CRASHOVERRIDE reports?
- Do you have a plan in place, with necessary resources identified, to address the risks like those identified by the InfraGuard and CRASHOVERRIDE reports? How is your Board involved and informed? Do you have experienced counsel to assist in that event? Do you or your counsel know, and have a relationship, with federal and state authorities who would be involved should there be a significant IIoT cybersecurity event?

Day Pitney's Cybersecurity practice group has established a working group focused on the IIoT. While this InfraGard and the earlier CRASHOVERRIDE warnings have been of primary interest to technical experts, such as chief information officers and chief information security officers (CISOs), they clearly warrant the attention of in-house counsel as well. While working to stay current on the constantly escalating risks and exposures, Day Pitney's Cybersecurity/IIoT working group has focused particularly on the legal issues implicated by the rapid expansion and significance of the IIoT for our clients. We will continue to provide reports, such as this, regarding the IIoT as appropriate and would be pleased to meet and discuss these issues with you.

---

[1] InfraGard is a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure. Day Pitney attorneys participate in InfraGard. More about InfraGard can be found here.

[2] A summary report has been distributed without dissemination restriction.

[3] See Day Pitney Client Alert, CRASHOVERRIDE, The Latest Malware Menacing the Electric Grid; see also US-CERT Alert TA17-163A, June 12, 2017

Authors

Naju R. Lathia

Partner

Parsippany, NJ | (973) 966-8082

nlathia@daypitney.com

Richard D. Harris

Partner

Hartford, CT | (860) 275-0294

New Haven, CT | (203) 752-5094

rdharris@daypitney.com