ALERT: Cyber Security Readiness Critical in Industrial and Manufacturing Sector

Advanced industrial manufacturing operations will become increasingly susceptible to cyber-attack.

While much attention has been paid to high profile cyber security breaches in the retail, healthcare, financial services and government sectors over the past two years, a relatively small number of cyber security incidents have been reported in the industrial manufacturing industry.

This won’t last, unfortunately.

Companies with advanced manufacturing operations continue to invest in highly integrated, smart, and interconnected systems to improve manufacturing performance and intelligence sharing across their respective supply chains. Bringing these systems together in a seamless system could increase the risk that one or more elements in the collection of systems and networks will become susceptible to unwanted intrusions and worse.

> *We are already seeing breeches in consumer oriented settings, products and environments. But the bigger cyber security challenge looms in loT, and this will likely occur in industrial and manufacturing environments.*

The signs of this are everywhere with cyber breaches an almost daily occurrence. Now the world is embracing the “Internet of Things” (IoT) in which virtually every device, system, appliance, car, patient bio bracelet—you name it!—will be stuffed with chips and software that will allow objects of all sizes and stripes to communicate and be engaged for operational and/or diagnostic purposes. Your car engine will tell its manufacturer it needs oil or a new gasket before you even know the engine is experiencing trouble. You will find out when the service manager calls your cellphone and advises you to drive your car to the nearest dealer for a quick check.

We are already seeing breaches in consumer oriented settings, products and environments. But the bigger cyber security challenge looms in IoT, and this will likely occur in industrial and manufacturing environments. Although manufacturing businesses have been implementing sensors and computerized automation for the past 20 years, the sensors, programmable logic controllers, PC-based controllers, and production control systems have largely been independent and separate from other internal business systems and external networks. This helped organizations to keep crooks locked out because entry was closed and less susceptible to hacking.

Today the closed legacy architectures of old are rapidly transforming into open, highly connected IP network architectures as businesses expand their investments in IoT, which is widely seen as critical to smarter, well-networked and communicative manufacturing. According to the United States Computer Emerging Readiness Team, the number of cyber security incidents reported by US federal agencies from 2006 to 2012 had grown by 782%. This is likely a reflection of more open and interconnected solutions being deployed in the industry. Meanwhile, IoT adoption in industrial manufacturing is accelerating. Gartner says there will be nearly 5 billion connected things in 2015. This number is projected to increase by five times over the next five years, Gartner says. In a survey by Tata Consulting Services of 13 global industry groups across North America, Europe, Latin America, and Pacific regions, industrial manufacturing companies reported the largest average revenue increase from IoT initiatives in 2014. Of the more than 3000 executives surveyed in the Tata study, 79% said they had IoT initiatives already in place today. The largest global industrial manufacturing companies such as GE and Caterpillar have already embraced IoT initiatives in a major way and very successfully.

Why are manufacturing operations at greater risk than they were in the past?

Ten years ago real-time production control systems were typically built in-house or through vendor technology-solution development. Most of the production control systems ran separately from other external networks or even internal company enterprise business systems. Over time, senior management faced an increasingly competitive global landscape and demanded real time integrated data for analysis, decision-making, and reporting. And they wanted—indeed needed—this information spanning their entire supply chains. This has led to the evolution and transformation of operations from isolated proprietary control systems to collaborative interconnected solutions that also rely on external integration with outside sources. Further complicating this structure of operation, surveillance and maintenance is the move to open systems and mobility: Industrial companies are moving from isolated control systems architecture to a more open system architecture involving the use of IP-based, wireless, and mobile devices. Such investments in more open, collaborative system architectures have clearly resulted in improved profitability and performance for the companies that adopt such change, but the move raises the bar for better security.

Why will the industrial sector become more vulnerable to cyber-attacks as the investment and adoption of IoT continues to expand?

The rapid development of all types of smart sensors that control outcomes and collect all types of data, combined with new levels of processing power, in a global network infrastructure connecting the world, has combined to make the IOT concept an attractive and affordable reality. The new sensors being developed are able to collect and share large amounts of data. The kicker and risk is that the industrial companies are now able to collect and share all types of data that is accessible across a broad network of users across their entire supply chain. This poses several unique and new cyber security challenges associated with IOT adoption in the industrial sector.

- There are risks associated with using old and new sensor technology in IOT solutions.
  Sensor technology has been around for quite some time just not at the scale it is fast becoming. Large industrial manufacturing companies use sensor technology on a significant scale in their industrial control systems. However, integrating the existing old sensor technology into new IoT solutions could leave a company wide open to cyber-attack as old sensor technology typically was designed with minimal cyber security protection, given the closed nature of the environments in which the sensors were implanted.

- As industrial companies expand their IoT, they are now embracing processes and systems to communicate and interact directly with outsiders such as vendors, contract manufacturers, and other third parties in their supply chains. This will increasingly make any of those connected more vulnerable to the weakest (cyber security) link in the supply chain.

- Unlike manufacturing, the financial services sector was one of the first business sectors to develop robust cyber security defenses and proactive and comprehensive incident response programs. Financial services companies over the past 10 years have deployed significant resources and investments in cyber security out of necessity. Now that the Industrial sector is expanding aggressively into the digital and highly connected world of IoT, it too will need to invest resources and talent to secure its businesses, assets and customer records in the open new world of IoT.

  This world of cyber intrusions will stand for nothing less.

Hugo Fueglein is a Managing Director in Diversified Search's New York City office. He is the leader of the CIO & IT Management Practice in the United States and is a core member of the Global CIO Practice for Diversified Search. Mr. Fueglein is also a leading member of the Global Technology Practice at Diversified Search.