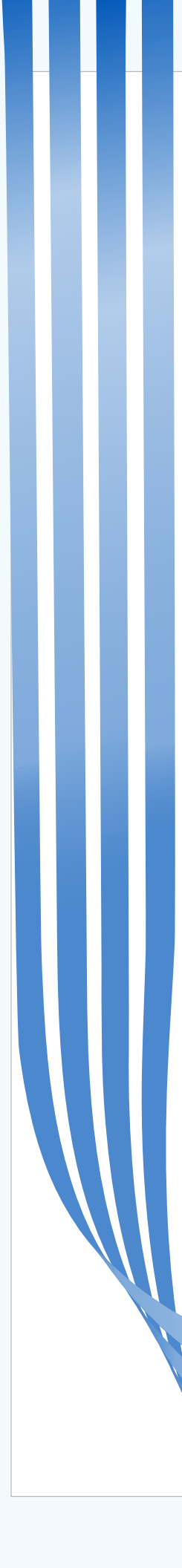


ARCH PERSPECTIVES

How **Cyber Risk** in Manufacturing is Evolving in Unexpected Ways



Pursuing
Better
Together®



New technologies like the Internet of Things (IoT) are changing the game for manufacturers, enabling increased efficiencies and making facilities safer, but are also exposing the industry to a number of new, unexpected risks. For instance, companies now need to think about everything from potential leaks of personal employee data to damaging hacks that can bring production at connected factories to a halt. This extends to bodily injury as well, which can potentially be caused by a cyberattack. Suddenly manufacturers are facing potential property damage, on-premise injuries and other “real world” implications due to cyber intrusions.

What now?

How Cyber Risk in Manufacturing is Evolving in Unexpected Ways

By Shiraz Saeed

Not too long ago, digital communication was effectively limited to laptops and mobile devices. But now, everything from your car, to your smart home, to healthcare monitoring equipment, agricultural harvesters and more are part of the internet of things (IoT), allowing them to communicate and share data over the global network without requiring direct human interaction.

And this is just getting started.

According to Statista, we're on track to see more than [30 billion](#) active IoT devices by 2025, up from barely 800,000 in 2010 and less than 14 billion in 2021. Not only is this explosion in connectivity changing what's possible from a hardware standpoint, extracting billions of data points from every single activity that happens on the IoT every day, but it is creating a new landscape of data-driven decision making that has broad implications across a wide range of industries.

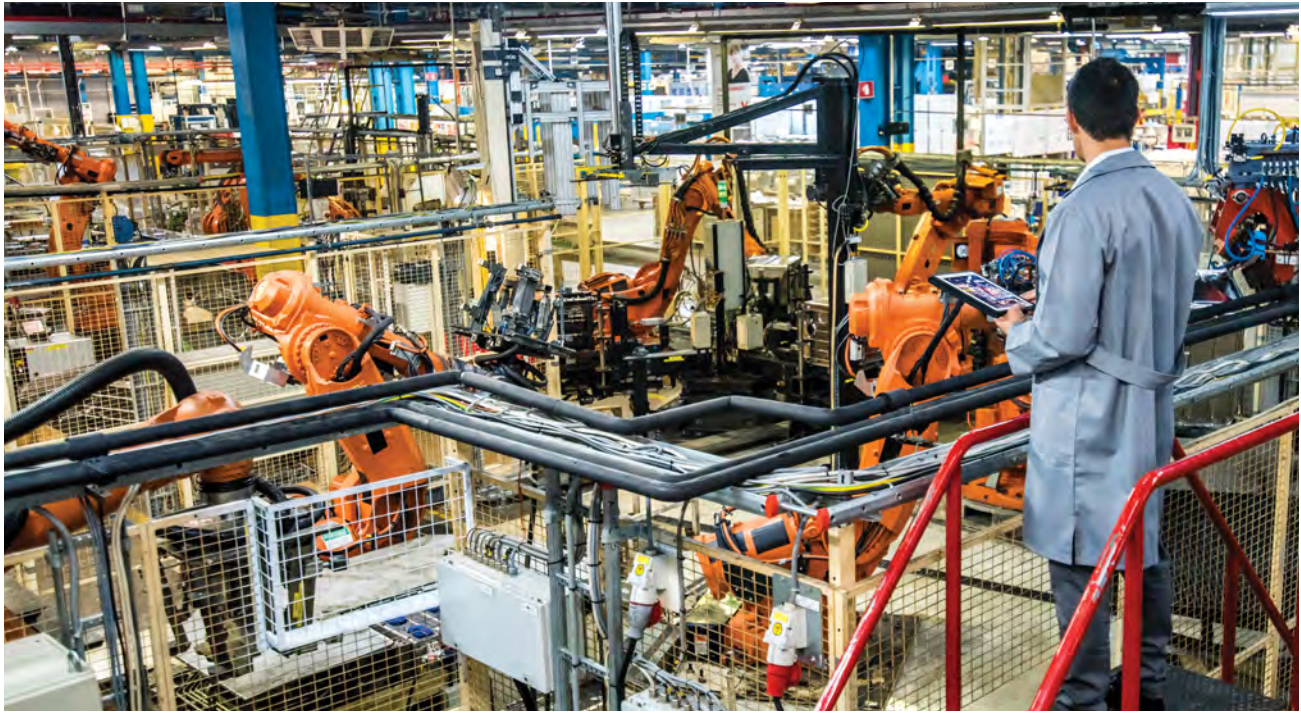
A game changer for manufacturers

One sector that is being particularly transformed by the growth in IoT is manufacturing, which long ago embraced innovations in robotics, labor efficiency and more. Incorporating digital connectivity into these existing processes is just the next step in this evolution. Broadly referred to as Industry 4.0, or the Fourth Industrial Revolution, this shift toward smart factories is making manufacturing facilities more efficient, safer and capable of producing far more at lower cost. In this context, IoT is often referred to as the Industrial Internet of Things, or IIoT, and extends to heavy equipment such as valves, production lines, pumps and more.

For those reasons, manufacturers of all types have been quick to adopt these technologies, with 90% of the industry [telling PwC](#) that they believe that digitizing their production processes will bring them long-term benefits and a full 98% expected to increase overall efficiency through digital technologies such as integrated manufacturing execution system software (MES), predictive maintenance and augmented reality. More than half of manufacturers view IoT as a key part of this [digital transformation](#), and 35% are already collecting and using data from smart sensors to [improve their day to day operations](#).

According to some estimates, Industry 4.0 as a whole could be worth as much as \$305 billion by 2030 as more and more manufacturers embrace the power of digital technologies to both remain competitive and carve out an advantage versus their competition. This includes producers as well as tangential industries such as those involved in warehousing, supply chain management and other related fields, all of which are seeing broad changes as a result of digital transformation.





Smart factories, new risks

But, the broad embrace of IoT and other technologies in manufacturing is exposing the industry to a number of new, unexpected risks, particularly when it comes to cyber.

Until recently, cyber risk might have been contained to the IT department and the software and hardware systems it uses to manage the company's data. But now IT is just one part of the full risk landscape. All of the other technologies used by manufacturers to control, track and process real-world devices – collectively known as Operational Technology (OT) – are equally important cyber risks that need to be addressed on their own, just as IT has always been. It's no longer enough to purchase cyber coverage for your data and call it good. Given the preponderance of IoT and OT systems in manufacturing, that is now only the beginning.

For instance, a connected factory that can communicate and share data with outside users is suddenly facing a long list of new cyber risks, ranging

from funds transfer fraud, leaks of personal employee data to damaging ransomware attacks that can impact operational technology and bring production to a halt. Maybe biometric data is being used for payroll and employee tracking, which can open the door to unintended privacy exposures. Whatever the technology being used by manufacturers, it is exposing these firms to cyber risk in new ways that can be easy to overlook.

From an insurance perspective, most cyber coverage traditionally revolves around two major concerns: network security and privacy. A network security breach involves the failure of an organization to protect its computer systems from unauthorized access, transmission of malicious code, ransomware, etc, while privacy refers to the failure to protect confidential, private, or sensitive personal or business information. Both can be mutually exclusive or intertwined and can cause significant problems for manufacturers from an operational perspective as well.

But today's manufacturers face another level of risk related to their cyber exposures.



Consider the possibility of bodily injury or property damage in a factory. That's not too far-fetched, as manufacturing work can be quite physical and hands on for employees. But what happens when a physical injury or damage occurs as the result of a network security breach? Maybe hackers take over some of the facility's IOT connected machinery and cause it to malfunction in a way that damages property and injures an individual. Suddenly the company is facing an on premise injury, property damage, and other "real world" implications following a cyber intrusion. Who pays for all that? Which insurance policies would respond? The responses to these questions are still a challenge. It depends on an organization's risk profile to properly be prepared for all of the potential liabilities associated with its digital transformation.

It can be possible for General Liability or Property policies to contain cyber coverage restrictions or exclusions. In an increasingly digital industry, the risk of a cyber event bleeding over into BI/PD territory is very real, requiring creative risk managers to look for new ways to protect their operations.

Addressing cyber risk for manufacturers

Manufacturers are today living in a new reality of cyber risk, grounded in their embrace of digital

technologies. As a result, it is increasingly important for the industry to adjust its thinking around cyber risk and where its liabilities truly lie.

The challenge for manufacturing now is to think outside the box and consider the true scope of the cyber risk it is now facing as a result of the industry's ongoing digital transformation efforts. There are simply too many potential pitfalls to ignore and too much on the line for those that fall victim to a cyber-attack.

Brokers and clients need to be asking tough questions: What systems, platforms or applications do we rely upon to operate our business? What other organizations do we rely upon to conduct our business? What happens if the systems, platforms or applications are not available for days or weeks? What plans do we have to maintain continuity and recover from the disaster? What happens if someone gets hurt as a result of a network security breach? What if data impacted by ransomware is exploited by bad actors? How much damage can a cyber-attack do to the overall operation?

The manufacturers that are best able to answer those types of questions are those that are best prepared to weather the new reality of the cyber risks facing the industry. ■





Shiraz Saeed

Shiraz Saeed leads the Cyber Risk product for Arch Insurance Group. Shiraz is responsible for the strategic direction for the underwriting, distribution and marketing of the Cyber Risk products and services offered by Arch. Shiraz joined Arch in 2021 and has over 10 years in the Cyber Risk industry. Prior to joining Arch, Shiraz had obtained a B.A in Finance from Hofstra University and an MBA in Strategic Management from Pace University. He started his tenure in the insurance industry within the professional liability division of American International Group (AIG) and quickly progressed to be part of the Cyber Risk product team responsible for the east coast territory. Most recently Shiraz was the Practice Leader for Cyber Risk at Starr Global Insurance, where he oversaw the strategic direction for their Cyber Risk products and services. With his extensive experience Shiraz is able to help stakeholders both internally and externally better understand the complexity of Cyber Risk, while also working with them to create solutions to help manage it.

Shiraz Saeed
Vice President, Cyber Product Leader
D: 914 216 7248
ssaeed@archinsurance.com

Arch Cyber

Arch Insurance is a leading global cyber insurer backed by more than a decade of cyber experience. We are technical underwriters with appetite for risk that allows an ease of business for our broker partners, their clients and our policyholders. We are creative and solution-oriented, and we want to be your go-to cyber insurance solution provider.

Arch Insurance

Arch Insurance is a market-leading insurer, providing a wide range of property, casualty and specialty insurance options for corporations, professional firms and financial institutions across the U.S. Our approach to doing business is based on collaboration, responsiveness and commitment. Together with our business partners, we pursue better ways of doing things and designing more effective solutions to respond to the needs of our customers.

©2023 Arch Capital Group Ltd. All rights reserved. This article is being provided to you for informational purposes only. Your use of this article, and all information and content contained herein, is at your own risk and is provided on an "as is" and "as available" basis. Arch makes no representations or warranties of any kind, express or implied, regarding the adequacy, validity, reliability, or completeness of this article. This article is not intended to imply or guarantee coverage under any policy of insurance, and Arch undertakes no duty to you by providing this article. The duties and liabilities of Arch are limited to those contained in its insurance policies.

Pursuing
Better
Together®

Learn More About
Our Cyber Solutions

