IIoT - THE FOURTH INDUSTRIAL REVOLUTION AND THE ONSET OF UNFAMILIAR RISK EXPOSURES

By: Alex Johanek, Risk Consultant, AHT Insurance

AHT INSURANCE

IIoT - THE FOURTH INDUSTRIAL REVOLUTION AND THE ONSET OF UNFAMILIAR RISK EXPOSURES

Did someone say the Fourth Industrial Revolution? Yes, but let's back up a bit to make sure we're all on the same page.

THE INTERNET OF THINGS (IoT)

The Internet of Things (IoT), explained in short, is the ever-growing network of devices that are connected to the internet. It used to comprise electronics, such as computers, smartphones and tablets. However, as a society, we have recently been welcoming a much wider array of internet-connected devices into our day-to-day lives. From smart TVs, thermostats and security cameras to washing machines, fitness trackers and smartwatches, the list of internet-connected devices continues to grow at a rapid pace. This network is what people refer to as the IoT.

SO, WHAT IS THE INDUSTRIAL INTERNET OF THINGS (IIoT)?

The Industrial Internet of Things (IIoT or Industry 4.0) is essentially IoT in a different environment. Specifically, the IIoT is the utilization of the IoT to improve manufacturing and other industrial processes via internet-connected machinery, sensors, robotics, vehicles, inventory management systems and even devices that monitor workers' vital signs.

Being able to gather and share data throughout your processes and control your operations remotely brings a variety of benefits to the industrial sector. For example, heat and vibration sensors that continuously monitor machines and provide necessary alert notifications facilitate predictive, preventative maintenance. Monitoring production lines throughout the entire process allows for deeper efficiency analysis, as well as provides better insight into lagging subprocesses and the adaptations necessary to account for those lags. Internet-connected inventory management systems and supply chains create opportunities to better manage inventory, materials and components. Speaking of components, do not forget 3D printing, also known as additive manufacturing, which can be used to print new and replacement parts when needed with no waiting for a shipment.

The transformation that IIoT (or Industry 4.0) is bringing to industrial processes, such as manufacturing, is so significant it is actually triggering what will be recorded in history as the fourth industrial revolution, hence Industry 4.0.

INDUSTRY 4.0 - THE FOURTH INDUSTRIAL REVOLUTION

Yes, we are already in the fourth era of the industrial revolution. Where did we start, and where are we now? First, there was the invention of the steam engine paired with mining coal in mass, which brought on mechanical production and more efficient transportation, like trains and steamboats. Second, there were scientific advancements and the beginning of mass production, including assembly lines, gasoline engines, advancements in chemistry, automobiles and airplanes, to name a few. Third, there was the digital revolution, spurred by electronics, computers, automation, programmable logic controllers and robots. Now, we find ourselves amid the fourth industrial revolution, which is being triggered by things such as IIoT, artificial intelligence, big data analytics, cloud computing, virtual reality and more. While it is exciting to witness, and be part of, the implementation of these industry-disrupting innovations, there are concerns that many businesses are not prepared to handle the inevitable onset of new, unfamiliar risk exposures.

NEW RISK EXPOSURES? LIKE WHAT?

For many years, the manufacturing and industrial processes space has been keenly aware of the importance of safety and risk management. Businesses in this sector are familiar with identifying and managing the current risks associated with their products, employees, operations, services, machines, sensitive data and a variety of other things. What they may be less familiar with, however, is what new risk exposures exist from the emerging trends in their industries and how to manage them.

One such trend is dramatically increased dependence on IIoT devices. Having more and more processes and information connected to the internet broadens a business's risk profile significantly, often into unfamiliar territory. For example, from a cybersecurity standpoint, manufacturers are becoming more and more aware of the need to protect their data and their customers' information. Often, they handle this by implementing cybersecurity measures (sometimes performed internally, other times provided by a consulting firm) then purchasing cyber insurance to protect themselves if their shield fails and there is a data breach.

While this is a good step, there are two major flaws with this approach. First, there is a disconnect between the implementation of cybersecurity measures and the procurement of cyber insurance. Party one provides cybersecurity services. Party two provides insurance coverage to protect against failures of the cybersecurity services. This context implies that cybersecurity and cyber insurance are independent, when they are meant to function symbiotically. So, why is it common for businesses to have two separate parties, who aren't in communication with each other, provide two interdependent parts of the cyber-risk management platform? There are companies that offer both cybersecurity resources and consulting, as well as cyber insurance coverage. Having one party, or at least communicating parties, work to provide both cybersecurity services and cyber insurance creates a more efficient and holistic cyber-risk management platform.

The second concern with the common approach to cyber-risk management is on the insurance side. A large focus is on covering data-related breaches, and it is extremely uncommon for a cyber-insurance policy to cover damage to property and people. The importance of having a cyber-insurance policy that also covers property damage and bodily injury may seem cryptic at first glance, so here are examples to provide some clarity.

What happens if a cybercriminal tampers with the functionality of an internet-connected safety mechanism? If a presence-sensing device, such as a light curtain, was tampered with and did not detect a worker, it could easily lead to injury or even death. Or, a cybercriminal tampers with a machine that has a heat sensor intended to shut it down when an unsafe temperature is reached. Tampering with a heat sensor's tolerance could cause a fire, explosion and even injure or kill bystanders. Suddenly, you have both property damage and bodily injury occurring from the same cyberbreach.

For a lot of businesses, having a cyber-insurance policy that covers bodily injury and property damage is critical. So, why is it uncommon for a cyber-policy to cover bodily injury and property damage? Inefficiencies are inevitable when industries are disrupted by emerging trends. Businesses are forced to work in ways they are not used to – leaving them unsure about how to properly manage the risks associated with their new activities. When this happens, education about the new risk exposures and changing outdated risk management methodologies becomes necessary to help stabilize their growth and protect their assets and longevity.

Alex Johanek is a Risk Consultant with AHT Insurance, a full-service insurance brokerage and consulting firm offering property and casualty, employee benefits, retirement, private client and international services for clients throughout the United States and 42 other countries. AHT boasts a nationally recognized manufacturing practice, led by Principal and SVP, George Forrester, with professionals who are leading experts in global industrial manufacturing risk management. Our dedicated team of insurance experts has invested years into learning the industry, understanding the risk exposures and working with insurance carriers and clients to create effective insurance and risk management programs.

AHT INSURANCE
ahtins.com | manufacturing@ahtins.com

AHT
INSURANCE