Why and How Manufacturing Needs to Take on Cybersecurity Today

In a report by The Balance, manufacturing in the United States was estimated to be worth $2.33 trillion last year – driving 12% of our national economic output. This industry employs 12.75 million Americans or 8.5% of the total workforce. Apart from being vital to the U.S. economy, the manufacturing sector has also been highly vulnerable to cyberattacks in recent years.

The Why: The Manufacturing Industry vs. Cybercrimes

Although the industry had previously escaped being affected by the biggest cybersecurity threats in the last decade, this all changed in 2017. That was the year that ransomware Wannacry and NotPetya – linked to China and Russia – locked computers that ran Windows and asked for cryptocurrency as payment. And even though the manufacturing industry itself wasn't the intended target of either ransomware, the attacks nonetheless resulted in massive losses in the industry. The losses came in the form of interruptions that were considered "catastrophic" by manufacturing giants like Mondelez in the U.S. and Reckitt Benckiser in Europe. Meanwhile, international pharmaceutical manufacturing company Merck cited losses amounting to $260 million that year. In its SEC filings, the company also mentioned that they expected additional losses of $200 million the following year.

In short, even just unintended, collateral cyber damage has already cost the manufacturing industry hundreds of millions. How much more damage can the world's best cybercriminals cause if they do decide to attack manufacturing head on? This is even easier to accomplish due to today's heavily digitized manufacturing processes. Like most other industries, manufacturing is becoming reliant on cloud data storage, which Tech Republic explains is the biggest new area of cyber vulnerability for the industry. Apart from getting their data stolen, manufacturing companies that store sensitive data in the cloud are also vulnerable to interruptions to business processes via database hacking.

The How: Getting the Right Cybersecurity Professionals/Software Your Team Needs

All of this has no doubt contributed to the increasing demand for cybersecurity professionals. In Maryville University's assessment of the cybersecurity industry they note that in 2016, the predicted shortage of cybercrime professionals was 1.5 million. That number has now doubled, as eSecurity Planet reveals that the current global cybersecurity staffing shortage has grown to 3 million. North America alone accounts for 500,000 of that 3 million, which reflects the

growing global demand for competent IT security professionals. This is, of course, good news for those seeking work in the industry, as they'll have plenty of options to choose from. Additionally, this growing demand is a good sign that the biggest movers in the industry are not taking cybersecurity threats lightly. In short, these numbers are highly indicative of the growing role that cybersecurity experts play, not just in manufacturing, but also in other industries.

By ensuring that they hire competent cybersecurity professionals, manufacturing companies will be able to identify any foreseeable flaws in their own cybersecurity infrastructure. For instance, the increase in manufacturing tech powered by the Internet of Things (IoT) presents many other vulnerabilities for hackers to exploit. Here at Mars International, we have already tackled how to identify critical security flaws that can be put down to companies' increasing reliance on connected technologies. The reality is that for today's tech-dependent manufacturing companies, streamlining and efficiency comes at the cost of cyber vulnerability.

As an industry that relies heavily on technology, the manufacturing sector faces many challenges, as well as several opportunities, in the face of today's cyber threats.

Cybersecurity Article composed by **Rian Judd** for **marsint.com**

Rian Judd is a writer who specializes in cybercrime and security. Her interest started after she graduated from university and she now devotes her time to finding the latest trends and information on the subject. She believes that her articles will help individuals and businesses improve the cybersecurity defenses.