CYBALT

Industry 4.0 Cyber Security Challenges – How real it is?

Cybalt Inc. Suite #510, 2701,
North Dallas Parkway, Plano, TX

discover@cybalt.com

Industry 4.0 Cyber Security Challenges – How real it is?

Many times “Industry 4.0” is considered just as a flashy catchphrase but many knows that it is a confluence of trends and technologies which promises to reshape the way things are made. In this article we will focus on knowing what Industry 4.0 is and then look at some of the key Cyber Security challenges associated with it.

Many are sceptical or still confused about “Industry 4.0” term. If you have a closer look at what’s behind Industry 4.0; it reveals some powerful emerging currents with strong potential to change the way factories work. It may be too much to say that it is another industrial revolution. But call it whatever you like; the fact is, Industry 4.0 is gathering force, and executives should carefully monitor the coming changes and develop strategies to take advantage of the new opportunities.

Start with some definitions. We define Industry 4.0 as the next phase in the digitization of the manufacturing sector, driven by four disruptions:

1. The astonishing rise in data volumes, computational power, and connectivity, especially new low-power wide-area networks.
2. The emergence of analytics and business-intelligence capabilities.
3. New forms of human-machine interaction such as touch interfaces and augmented-reality systems, and
4. Improvements in transferring digital instructions to the physical world, such as advanced robotics and 3D printing.

(The four trends are not the reason for the “4.0,” however. Rather, this is the fourth major upheaval in modern manufacturing, following the lean revolution of the 1970s, the outsourcing phenomenon of the 1990s, and the automation that took off in the 2000s.)

Most of these digital technologies have been brewing for some time. Some are not yet ready for application at scale. But many are now at a point where their greater reliability and lower cost are starting to make sense for industrial applications. However, companies are not consistently aware of the emerging technologies. We surveyed 300 manufacturing leaders in January 2015; only 48 percent of manufacturers consider themselves ready for Industry 4.0. Seventy-eight percent of suppliers say they are prepared.

Cybersecurity as a key enabler of adoption:

There’s a lot to be gained by adopting Industry 4.0 technologies, so why hasn’t adoption kept pace with expectations? The answer is simple: security.

As it continues to adopt Industry 4.0, the manufacturing industry becomes an increasingly appealing target for attackers, who have the opportunity to move laterally across a manufacturing network, jumping across IT and OT systems for their malicious activities. Without strong protections in place, bad actors can take advantage of systems for industrial espionage, intellectual property theft, IP leakage, or even production sabotage.

Industry 4.0 cybersecurity challenges:

Manufacturing is the second-most attacked industry, yet the manufacturing sector lags when it comes to security.

Smart factories can be subject to the same vulnerability exploitation, malware, denial of service (DoS), device hacking, and other common attack methods that other networks face. And the smart factory's expanded attack surface makes it extra difficult for manufacturers to detect and defend against cyberattacks. These threats now work on an entirely new level with the dawn of the IoT, and they can result in serious physical consequences, especially in the realm of the IoT.

Here are a few new security challenges that organizations face in the age of Industry 4.0:

- Every connected device represents a potential risk.
- Manufacturing systems such as Industrial Control Systems (ICS) have unique vulnerabilities that make them particularly susceptible to cyberattacks.
- Industry 4.0 connects previously isolated systems, which increases the attack surface.
- Upgrades are often installed piecemeal since the systems are very complex.
- Manufacturing has many fewer regulated compliance standards than other sectors.
- Visibility is poor across separate systems and isolated environments.

Also, note that the battle is decidedly unbalanced. While organizations must protect a wide swath of technology over a very large attack surface, attackers need only pinpoint the weakest link.

In the end, security best practices will be key to the success of Industry 4.0. The manufacturing sector needs to Adopt a risk-based security mindset (tying business criticality to defence strategies), Keep an accurate inventory of all OT assets in real-time, Marry the best of IT and OT as an integrated defence strategy across all attack surfaces, Identify and fix outdated systems, unpatched vulnerabilities, and poorly secured files, Take a security-first approach to the deployment of new connected systems. Remain ever vigilant to spot potential threats with real-time vulnerability assessments and risk-based prioritizations, Ensure that technology suppliers and connected equipment manufacturers commit to regular security and software patches and audits, Threat intelligence, including monitoring of the dark web, can also act as an early warning system to uncover planned attacks. Thus, the organization can pre-empt a breach and take immediate action to protect their digital corporate assets and physical infrastructure.