Security and threat's in Industry 4.0

Dr. Biju Nathan
EbixCash Financial Technologies

***Abstract*- ICT has brought in lot of advancement in manufacturing industries with technology. It has helped in best use all the resources involved in production. However, with use of new technologies and new threats have come. This paper focuses on Industry 4.0 and security threats and how to deal with the threats.**

Index Terms- Compressive Sensing, Data Gathering, Random Walk, Wireless Sensor Network

I. CURRENT WORLD SCENARIO

Information and Communication Technologies (ICT) has become part of day today life, example it helps to connect with each other through emails, call and chats. ICT is a combination of computer information and telecommunications technologies, and their applications. ICT supports various industries because the IT revolution has brought an important transformation with new technological solutions and high impacts. With advancement in technologies we have the new technology journey as below:

- Emergence of cloud-based systems
- Internet of Things (IoT)
- Big Data
- BYOD (Bring Your Own Device)
- CYOD (Choose Your Own Device)

II. THE INDUSTRY

The growth of Industry over the last few hundred years have taken the manufacturing production to a new level where the production is currently controlled based on Information and Communication Technologies (ICT). The current devices are controlled by IT devices. They are also automated so involvement of Human is least, this is being done to ensure less errors and improved efficiencies in production. This has helped to accelerate the production and time. The investments are more as compared to traditional models however the cost advantage is better.

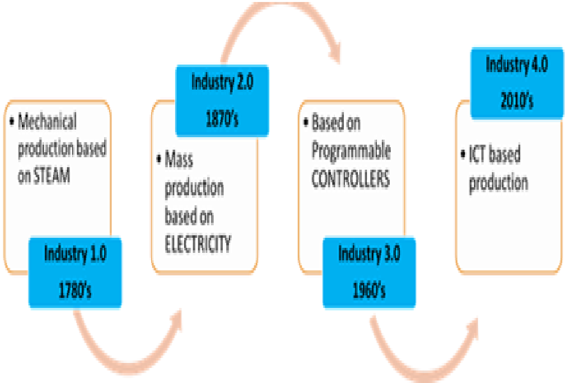
• Mechanical production based on STEAM
Industry 1.0
1780's
Industry 2.0
1870's
• Mass production based on ELECTRICITY
• Based on Programmable CONTROLLERS
Industry 3.0
1960's
Industry 4.0
2010's
• ICT based production

Figure 1Industry Revolution

As the industry expands, the number of security solutions available has exploded so that a recent study revealed that IT security professionals are struggling to keep up with the technologies that drive digital transformation.

Despite new offerings to enhance supply chains and digitalize customer experiences, new security challenges have unfurled in the form of an expanded attack surface. This is a double-edged sword and is increasingly becoming a boardroom issue.

How do companies keep up with the pace of innovation (and competition) while protecting their critical assets from security breaches?

III. IOT AND BENEFEITS

IOT (Internet of Things) is a bundle of devices working as a system which embeds with sensors, software, electronics and connectivity to allow it to perform better by exchanging information with other connected devices, the operator or the manufacturer.

It has brought new benefits for customers, by

1. Shortened production cycles
2. Incorporation of customer needs in real time
3. Maintenance is largely carried out automatically
4. Orders are automatically filled in the right order, shipped and dispatched.

The growth of IOT can be understood by the figure below: -

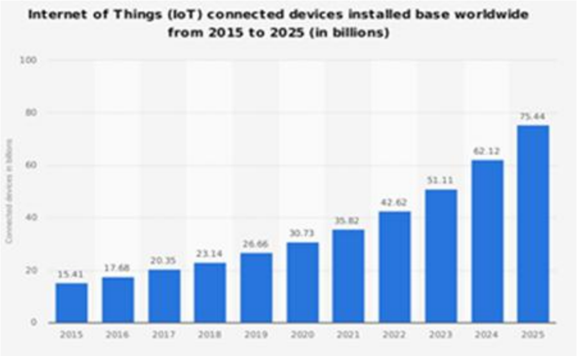

Figure 2Growth of IOT in the world

IV. WHY THERE IS GROWTH?

The growth in the industry with the use of current technologies is termed as Industry 4.0, this emergence of digital manufacturing or also named as "smart" factory, which means

1. Networking Smart
2. Mobility
3. Flexibility of industrial operations
4. And their interoperability, integration of customers and innovative business models

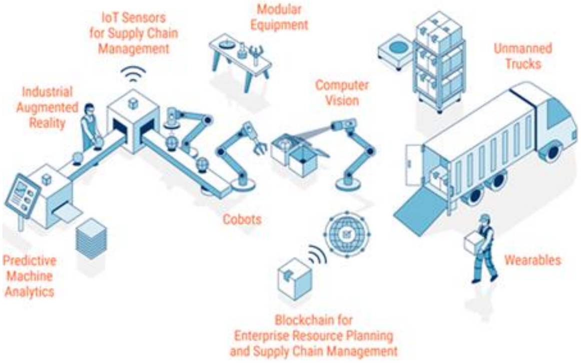
IoT Sensors for Supply Chain Management
Modular Equipment
Unmanned Trucks
Industrial Augmented Reality
Computer Vision
Cobots
Predictive Machine Analytics
Wearables
Blockchain for Enterprise Resource Planning and Supply Chain Management

Figure 3Smart Factory

1.Networking Smart

In current time the factories are networked by use of IT and now called as Smart networked factories. This facilitates the factories in "Plug & Work/play" mode with the help of synchronized networking, distributed processing capabilities, heterogeneous sensor interfaces and layered cyber-security. The internet technologies are used for logistics systems and operating supplies as well as automated systems and equipment.

This facilitates the accessibility to the resources used and a smart control, adding value to the business performance.

2.Mobility

The industries have gone mobile with availability and use of technologies using the Mobility which are driven by Smartphones and Tablets for industrial automation, it provide access to processes and services of the automated system. It helps in

- Easy diagnostics, maintenance and operation of these systems.
- Cloud-based platforms, to use system-based applications, real-time end-to-end planning and horizontal collaboration
- Integrated with horizontal value chain partners and customers. Thus, reduces inventories

Why Mobility?

The Global mobile usage data is growing day by data due to ease and competitiveness. Data growth in recent time can be measured Exabyte (EB), which is a multiple of the unit byte for digital information.

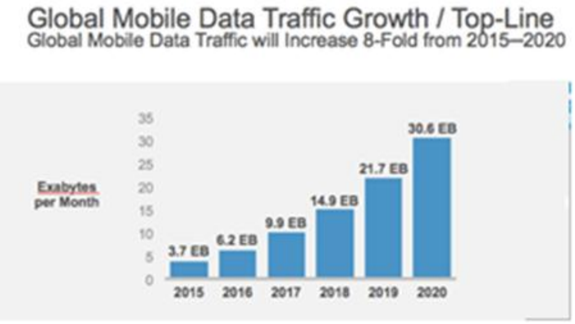

Figure 4Mobile Data Growth

Note:

The prefix Exa indicates multiplication by the sixth power of 1000 (1018)

1 EB = 1 million Terabytes (where 1000 EB = 1 ZB)

3. Flexibility and interoperability

The current technologies are more flexible and with interoperability. There are availability of large number of suppliers providing multiple components, modules and services. With the development of automated systems IOT is moving from proprietary to open standards-based solutions. This will facilitate the connectivity and interoperability between devices. Move away from proprietary designs (built on nonstandard communication protocols) saves cost and dependencies.

4. Integration of customers and Innovative business models

There is integration of customers and various business models happening in the industry, this is facilitated due to following reasons:

- Alignment of companies and costumers - through e-commerce, digital marketing and social media, and monitoring closely the costumers' experience and by Data collection and analysis
- Specific individual needs of customers by customized products due to Customer service, flexibility, efficiency and cost reduction
- Right product Quickly is happening due to Integration of the supply chain

V. SECURITY THREATS

The integration of new systems and their increased access raises new data security breaches.

By embracing the virtual route, organizations are presenting cyber-criminals with endless entry points into the system to cause disruption to the business.

There are few Risk as highlighted below:

1. Key assets were being stored and processed digitally, this made them more vulnerable to attack
2. Cyber-criminal's strategy is to identify a weak point and move laterally within an organizations system and exploit its data
3. Simply patching and mitigating vulnerabilities in inadequate
4. Lack of fully protected and transparency within the connected system(s)/organization(s)

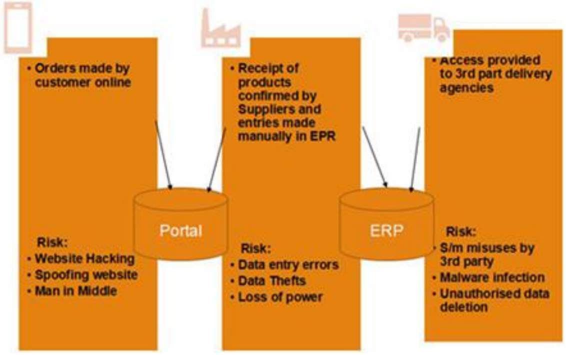
• Orders made by customer online
Risk:
• Website Hacking
• Spoofing website
• Man in Middle
Portal
• Receipt of products confirmed by Suppliers and entries made manually in EPR
Risk:
• Data entry errors
• Data Thefts
• Loss of power
ERP
• Access provided to 3rd part delivery agencies
Risk:
• S/m misuses by 3rd party
• Malware infection
• Unauthorised data deletion

Figure 5Security Risk in a Factory

The below are the security issues that is noticed in a Factory example as depicted in Figure 5:-

1. Enterprise Cyber-Spying/Espionage, Confidential Information and Intellectual Property
2. Denial-of-Service
3. Supply Chain and the Extended Systems
4. Smart Security and the Smart Factory

VI. SECURITY STEPS

The hackers are the one who have been taking advantage of Digital Transformation. If a full range of security best practices are properly operated, 24/7/365, then it is entirely feasible that an enterprise can remain secure. The reason why organizations get breached is because they leave gaps and cut corners, not because technological solutions are inadequate. Anti-virus technology may be left floundering now, blind to a significant minority of malware, but there are well-defined compensating technologies that will ensure 'broad threat spectrum' protection is provided.

That isn't the reality of the situation - most security breaches happen because they can take place. There are few steps that needs to be mandatorily taken by organizations, few of them are as follows:

1. Neglecting patching and system updates presents a huge window of opportunity for attackers, hence Patching the software used with the latest update is most important
2. Penetration testing needs to be carried out for the network and devices yearly to check the security issues. It would be an appropriate method to gain a holistic overview of the entire system. Highlight any vulnerable assets and uncover critical issues that could put the business at risk.
3. Attention on remediating issues based on risk levels which maximizes their time and efficiency. Address the findings from both a business and technical perspective.

Introducing automation within continuous security monitoring solutions can equally be beneficial and efficient to match the ever-changing techniques used by today's cyber-criminals

For any organization can implement the above 3 step as part of Industry 4.0 Security process to overcome the threats and move towards a Smart and Secured industry environment.

REFERENCES

[1] http://en.wikipedia.org/wiki/Information_security

[2] https://www.pcisecuritystandards.org

[3] https://www.owasp.org/