Cyber risks in Industry 4.0 – Digital Supply Chain

– Sudhansh Sharma
Assistant Professor, SOCIS, IGNOU, Delhi
sudhansh@ignou.ac.in

Article History
Paper Nomenclature:
Experiential Research Papers (ERP)
Paper Code: CYBNMV1N5OCT2019ERP2
Submission Online: 08-Oct-2019
Manuscript Acknowledged: 10-Oct-2019
Originality Check: 17-Oct-2019
Originality Test Ratio: 7%
Peer Reviewers Comment: 18-Oct-2019
Blind Reviewers Remarks: 19-Oct-2019
Author Revert: 22-Oct-2019
Camera-Ready-Copy: 25-Oct-2019
Editorial Board Citation: 28-Oct-2019
Published Online First: 31-Dec-2019

Industry 4.0 i.e. the fourth industrial revolution is dominating the evolution of traditional supply chain structure, by using the intelligent, interconnected platforms and devices i.e. using Internet of Things (IoT). This leads to the evolution of Digital Supply Chain (DSC) systems which are capable to manage the data dynamically i.e. capable of capturing data from points across the value chain and update the information at each point. This leads to better management of goods and flow of materials, much efficient use of resources, and supplies to meet customer needs[1]. But this digital connectivity among the supply chains, manufacturers, customers and operations; leads to higher risks posed by cyber security threats. The performed work relates to the study of the cyber risks faced by the Digital Supply Chains (DSC)[2]

Keywords : Industry 4.0 | IoT | Data Sharing | Block-Chain

Introduction:

The term Connected Industry relates to the fourth industrial revolution otherwise known asIndustry 4.0, focusses on the digital integration of people and machines with the internet and information technology. The consumers are in fact the key players in this concept of Industry 4.0, and the work of digital integration is facilitated to a greater extent by software-based systems. This digital integration involves the entire value stream. The flow of Information happens both vertically and horizontally, vertically from the individual components all the way up to the company's IT platform and horizontally between machines and the company's manufacturing system.

Internet of Thing (IoT) increased the connectivity of smart machinery, which raises the stakes of Industry 4.0. This heralds a new age of connected, smart manufacturing, along with responsive supply networks, and tailored products and services, through its use of smart, autonomous technologies. Industry 4.0 strives to marry the digital world with physical action to drive smart factories and enable advanced manufacturing.[3] This leads to better management of goods and flow of materials, much efficient use of resources, and supplies to meet customer needs[4]. But this digital connectivity among the supply chains, manufacturers, customers and operations; leads to higher risks posed by cyber security threats, for which the industry is unprepared. Developing a fully integrated strategic approach to cyber risk is fundamental to manufacturing value chains as they marry operational technology (OT) and information technology (IT)—the core driving force of Industry 4.0.

The supply chainmainly relates to the information regarding production and distribution viz.—how materials are entering into the production process, and whether the goods distributed outside are semi- or fully finished, such information is quite fundamental to any manufacturing organization, and highly related to the consumer demand. Many global organizations tales the help of forecasting techniques to perform the demand forecasts of the quantity of materials necessary forthe manufacturing line requirements, and distribution channel loads. Nowadays, Data Analytics have also become more sophisticated, and today's organizations are utilizingit to understand and predict the buying patterns. Thus, management and security of the enormous amount of data produced by DSC's is again very important because the Data Analytics of such data may leads to some

findings which may be a threat to the Cyber security for the smart industries, thus the cyber risk strategy is different in this age of Industry 4.0. When supply chains, factories, customers, and operations are connected, the risks posed by cyber threats become all the greater and potentially farther reaching.

The cyber risks of sharing data across the DSC

Evolution of the concept of DSC relates to the creation of a network that allows real-time, dynamic pricing of materials or goods based upon the consumer demand relative to the available supply of goods.[5] The network of such nature is possible only by using the concept of open data sharing among the participants in the supply network, but this may create significant hurdles, because it will be quite difficult to maintain the balance between data transparency and information security.

The Smart Organizations under industry 4.0 should work on the ways to secure the information from the unauthorized access, this involves the maintenance of the safeguards across all supporting processes, such as vendor acceptance, information sharing, and system access. The identified processes may be proprietary or they may also potentially serve as access points to other internal information, which may put more emphasis on third-party risk management. While,analysing the cyber risks of interconnected DSCs, it is observed that the two key cyber imperatives i.e. Data Sharing and Vendor Processing are the cyber imperatives, having the highest impact of the increased supply chain connectivity.In this paper we will discuss the cyber imperative areasi.e. data sharing and vendor processing, and the potential strategies for addressing increased cyber risks as well.

Data sharing: Increased access to data for more stakeholders

What data should be shared, and how to protect the systems and underlying data, that may be proprietary or have privacy risks, are the key concerns of the smart organizations under industry 4.0. For example, in a particular DSC, some suppliers may be competitors, and they may not wish to share certain type of data like product pricing or the information related to the proprietary materials. Further, the suppliers may be bound to some regulations that limit the type of information that can be shared. Allowing the access to just part of the data may make it possible for those with malicious intent to gain access to other information.To be on the safer side the Organizations should utilize good network practices such as network segmentation and usage of the intermediary systems to gather, protect, and provide information.

Internet of Things (IoT) devices are playing the key role to implement Industry 4.0 standards, thus the incorporation of the additional technologies like trusted platform modules and hardware security modules, to the future IoT devices is highly required. Provision of such technologies in the future devices will provide robust cryptologic support, hardware authentication, and attestation (that is, detect when unauthorized changes are made to the device). The combination of technological approaches leads to the development of secure application points and end points to protect the data and processes.

Indeed, organizations should perform risk assessments across their environment, including enterprise, DSC, industrial control systems, and connected products, and use those assessments to determine or update their cyber risk strategies. Taken together, all of these approaches can help to identify areas where higher levels of prevention which can be warranted, with the increase of the interconnected DSC's.

Vendor processing: Vendor acceptance and payment in a broader market

Vendor processing is the next cyber imperative, with an objective to maintain trust when processes cannot be validated, it is having the highest impact when there is a voluminous increase in the connectivity of DSC's. Breach in this cyber imperative i.e vendor processing leads to the entry of counterfeit goods and fake store fronts, which create headaches for organizations such as eBay and Amazon.[6]

This is the result of the enlargement of a core group of suppliers to a broader network, with disjoint vendor acceptance processes, because new partners generally comes up with their own systems into the existing mix of vendor processes. Thus, to be secure, it is very much required to develop new policies and guidelines for adequate security from fraudulent vendors, suppliers, and subpar product distributors. Further, the Governance, risk, and compliance (GRC) software are required to track the third-party acceptance and perform risk management.

Blockchain and Crypto Currency

Block Chain has been suggested as a technology to solve the identified cyber risks in the DSC's of Smart Organizations under Industry 4.0. The Block chain technology has potential to address issues related to payment process. The process of establishing a historical record for currency is best known in the example of Crypto Currency, now the organizations are exploring ways to use block chains to manage DSC's i.e. to determine the flow of goods from production line

through layers of purchasers.[7] Further, Creating a historical ledger that is shared by a community establishes trust and visibility, providing protection for buyers and sellers by certifying a good's authenticity, enabling the tracking of goods movements for logistical purposes, and categorizing products more specifically than by lots or batches when handling recalls or defects.[8] In the absence of this level of assurance of product authenticity, manufacturers may want to perform testing and certification of products to ensure adequate security before incorporating them into their environment or products.

Conclusion

It is the factor of trust that establishes the connection between these two areas i.e. data sharing and vendor processing. Digitization is the only hope to maintain the trust in the DSC's for Smart Organizations, which requires continuous risk management to preserve integrity and remain secure when transacting information or goods, across the network. Combination of secure IoT devices and Block Chain can strengthen the monitoring capabilities and cyber security operations, toprotect processes when trust cannot be validated.

References

- Giovanna, Fabio, Matteo, Marco; Addressing Industry 4.0 Cybersecurity Challenges, IEEE engineering management review, vol. 47, no. 3, third quarter, september 2019
- Mike Lackey, Industry 4.0 And The Digital Supply Chain, April 4, 2019 https://www.digitalistmag.com/digital-supply-networks/2019/04/04/industry-4-0-digital-supply-chain-06197590
- enisa, industry 4.0 cybersecurity: challenges & recommendations may 2019
- René Waslo, Tyler Lewis, Ramsey Hajj, Robert Carton, Industry 4.0 and Cyber Risk: Security in an Age of Connected Production, July 16, 2017; https://www.supplychain247.com/paper/industry_4.0_and_cyber_risk_security_in_an_age_of_connected_production/security
- For further information about digital supply networks, see Adam Mussomeli, Stephen Laaper, and Doug Gish, The rise of the digital supply network: Industry 4.0 enables the digital transformation of supply chains, Deloitte University Press, December 1, 2016, /content/www/us/en/insights/focus/industry-4-0/digital-transformation-in-supply-chain.html. View in article
- Trina Huelsman et al., Cyber risk in advanced manufacturing, Deloitte and MAPI, 2016,https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html. View in article
- Adam Mussomeli, Stephen Laaper, and Doug Gish, The rise of the digital supply network: Industry 4.0 enables the digital transformation of supply chains, Deloitte University Press, December 1, 2016, /content/www/us/en/insights/focus/industry-4-0/digital-transformation-in-supply-chain.html. View in article
- Harriet Green, "Serving up a better burger: How IoT and blockchain will reinvent the global supply chain," Venture Beat, October 30, 2016, http://venturebeat.com/2016/10/30/serving-up-a-better-burger-how-iot-and-blockchain-will-reinvent-the-global-supply-chain/. View in article

Dr. Sudhansh Sharma is a student of multiple disciplines viz. Computer Science, Physics, & Operation Research. His academic credentials involve following PhD (Physics),M.Sc.(Physics), M.Tech. (Computer Science), MBA(Operation Research). He has got one and a half dozen of Publications in various National and International Journals/Conferences. He is the Technical Reviewer of various Journals and Conferences of National and International repute. He tried to express his understanding of interrelation between Base sciences and Computer science through his Book "Modeling Of Novel MOSFET Devices – Basics, Concepts, Methods" published by Lambert Academic Publishing(Germany), and Contributed to an edited Book titled "E-Commerce and Online Banking", as an editor, published by Manakin Press, India. He has delivered invited talks in various Workshops, Refresher and Orientation programmes. His experience includes both, industrial and Academic Domains. He has been associated with various Industries and academic institutions. Currently he is serving as Assistant Professor in the School Of Computers and Information Sciences – IGNOU:

sudhansh@ignou.ac.in

Annexure I

Submission Date	Submission Id	Word Count	Character Count
08-Oct-2019	D61606918 (urkund)	2176	13154

Urkund Analysis Result

Analysed Document: 22Dec19_Evolving Cyber risks in Industry 4.docx (D61606918)
Submitted: 12/22/2019 8:53:00 AM
Submitted By: scholastic.seed@gmail.com
Significance: 7 %

Sources included in the report:

https://broadband-nation.blogspot.com/2019/11/industry-40-and-cybersecurity.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/QVdLeH+(BroadBand+Nation)&m=1

Instances where selected sources appear: 2

Note: Cybernomics runs an Urkund plagiarism tool for the originality check of an article before publication. Urkund is developed by Prio Infocenter AB based in Stockholm, Sweden.

Reviewers Comment

Review 1
This is Purely Experiment paper, it has a lot of facts on upcoming industry revolution 4.0. Value of Industry 4.0 comes from improving productivity and removing inefficiency at all levels, making it one of the most valuable ideas of our time.

Review 2
This is above the expected value of the Internet of Things (IoT) market, which Gartner has estimated will be worth almost US$3.7 trillion by 2020.

Review 3
It is aiming to construct an open, smart manufacturing platform for industrial-networked information applications.it is expected that it will come with massive industrial change.

Editorial Excerpt

Initially at the time of submission article has 7% of plagiarism which is satisfiable percentage for the publication based on a URKUND Plagiarism, The above article named "**Cyber risks in Industry 4.0 – Digital Supply Chain**, it illustrates about the upcoming Industry 4.0. The name given to the growing combination of traditional manufacturing and industrial platforms and practices with the latest smart technology.This primarily focuses on the use of large-scale M2M and Internet of Things (IoT) deployments to provide the likes of increased automation, improved communication and monitoring, as well as smart machines that can analyse and diagnose issues without the need for human intervention.Anything attached to the Internet of Things or increased automation is worth a tidy sum and Industry 4.0 is no different, with analysis valuing the technology around the idea as practically never-ending.On the basis of Examination on this article. It is earmarked and decided under the ambit of "**Experiential Research Papers (ERP)**".

Scholastic Seed Inc.
www.scholasticseed.in

Citation

Dr. Sudhansh Sharma
"Cyber risks in Industry 4.0 – Digital Supply Chain"
Volume-1, Issue-5, Oct 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.