SUPPLY CHAIN RESILIENCE AT THE APT COST AND EFFORTS THROUGH VISIBILITY

Deepika Aggarwal
Assistant Professor
Kautilya Institute of Management & Research
Jayawant Shikshan Prasarak Mandal, Pune
goel.mbadeepika@gmail.com

Dr. Poonam Singh
Assistant Professor
Kautilya Institute of Management & Research
Jayawant Shikshan Prasarak Mandal, Pune
poonam.b88@gmail.com

Abstract

The trade war between China and U.S. and supply and demand prostrations brought on by the covid-19 have been impelling the manufacturers everywhere to reappraise their supply chains. The vulnerabilities exposed from the wide spread of covid-19 has taught a lot of valuable lessons to Indian supply chain industry, particularly in formulating the supply chain strategies concentrating more on delivering quality despite the cost, including supply chain resilience. After covid-19, skilled labour shortage, manufacturing shifts from host countries to home countries, scarcity of resources with environmental threats, advanced persistent threats, technical disruptions, cyber-attacks and collapse of trust and visibility have emerged as the biggest challenges for SCM organisations. Overcoming the above-mentioned shortcomings, the resilience of supply chain has become the strong urge now-a-days for the SCM units with the need of re-imagining, re-thinking and re-managing the supply chains to ensure disruption free business continuity and progress with growth.

The supply traumatism that started in China in February 2020 and the demand collapse, that go around with, as the global economy abandonment laid bare fragility in the production strategies and supply chain organizations just about everywhere.

The trade diminution and meagerness of pharmaceuticals, with dyslogistic medical supplies and other necessities called attention to their weaknesses, which in turn triggered a revolt in economic nationalism. As a result globally, the manufacturers are running under extensive and fierce competitors' and political pressure, to enlarge their national production with increased employment in their own nations and to decrease or even eradicate their subordination on sources which are considered vague, vulnerable and even precarious and to rework on their lean manufacturing strategies which include decreasing the quantity of inventory stuck in the Global supply chains.

COVID-19 REVEALING THE VULNERABILITIES OF INDIAN SUPPLY CHAIN INDUSTRY

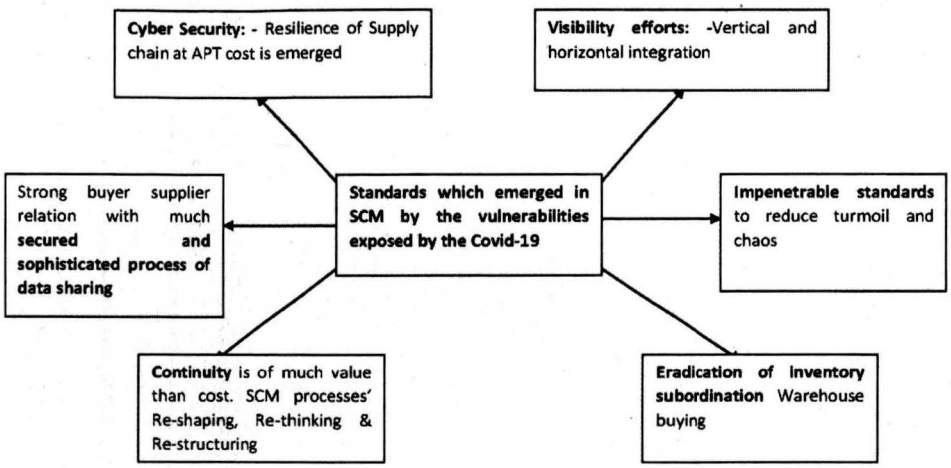
India being the country of high population with proportionately scarce pharmaceutical and health infrastructure was deeply impacted by mounting spread of covid-19 and left the Government of India helpless and compelled to pass an order for countrywide lockdown initially for 21 days in March 2020 and continued thereafter which brutally impacted the already struggling economy.

Even before the lockdown, the exponential spread of covid-19 had imposed grievous disruptions in China and virtually closed global trading. The vulnerabilities emerged from this undulated disruption led

many industries towards business closure and left no room for inventory bluffers.

The industries running under Chinese subordination for inventories were completely devastated and were brutally exposed the vulnerabilities of supply chains.

LESSONS LEARNT BY SCM UNITS FROM THE VULNERABILITIES EXPOSED BY THE COVID-19



Cyber security: A guide to supply chain resilience at APT cost

In the process of supply chain resilience with re-configuration and re-assessment, the security against cyber attacks is of prime importance requiring immediate attention. Let us s know the terms "cyber attack" and "advanced persistent threat".

Cyber attack is an attack on the cyber system of supply chain that seeks to ruin an organisation by picking out its less protected and endangered components. Predominantly, the cyber offenders interfere by constructing steps of a product by positioning a root kit perceiving constituents.

Advanced Persistent Attack is the attack of infiltration and penetration in your organisation by the digital cyber criminals to disrupt your specific and confidential data by gaining access in a very advanced and automated manner.

The attacks are orchestrated in such a sophisticated manner that the mitigation of attack possibility and detection of threat becomes very tough and complex.

Advanced :- Highly sophisticated hacking skills

Persistent:- Not a quick bug but a steady, spontaneous attack, orchestrated by cyber malware; the hacker didn't attack for a while

Threat:- To access and disrupt the confidential data

How does it work

Step:-1 Initial exploitation, reconnaissance & scrutinization, gaining access to the targeted company's network (access initiation)

Step:-2 Malware installation (bugs deployment)

Step:-3 Scrutinization search for other vulnerabilities in the targeted network

Step:-4 Expanded access infiltration and penetration in specific targeted data

Step:-5 Suction, exploitation and manipulation of confidential data (data theft)

Step:-6 Follow up removal of threat evidence

SOLAR WINDS (IT MANAGEMENT VENDOR) APT CASE

Recently a US based company SolarWinds Inc. that was in the business of developing software for businesses and also for the U.S. Federal Government, having a database of more than 3,00,000 customers, to help and manage their network, was being targeted by an attacker of Advanced persistent threat(APT). The outbreak of its cyber defense mechanism is the most poignant and sophisticated event of recent time.

How did it take place: - To distract the cyber system of SolarWinds, the advanced persistent threat criminal used the complicated Zero-day malware, which, when implemented on its developer system, would be able to recognise and could also wait until the developer retrieved the fixed code file. And then it started supplanting the source files and loading the malicious code into SolarWinds software and authorising its software updates.

This modus operandi of cyber attack is commonly known as attack on supply chain as it strikes on all inter-linked organisations using a most trusted software infected by malware.

The complexity of exposing and countering the attack:- A threat detection servicer, Firewalls and other investigating organisations were contestably meagered in its potentialities in exposing the attack. Reports indicated

The mostly used software to enhance the visibility, now a days, mainly by apparel retailers globally is Radio Frequency Identification Technology (RFID)

that the attack might have begun in early September 2019, but the whole incident reached to cardinality in Dec.2020. Till then all customers of SolarWinds were subject to that exposure for a couple of months, until the whole incident became public.

Hence the CISO's must know that they should have a sound system and processes of supply chain management and should have in place a mature change management processes. However considering the complexity of this cyber attack on supply chain it is worthwhile to consider if traditional supply chain management practices are adequate enough to address such issues like SolarWinds cyber-attack.

OTHER APT ATTACKS ON SUPPLY CHAINS

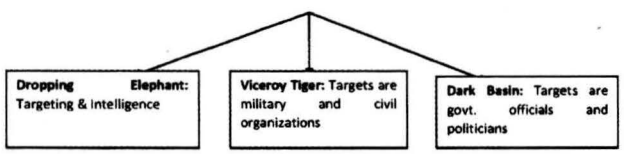
APT attack on Marriot Hotel of StarWood Hotels group: Extremely sensitive information of 339 million guests was breached. The Hotel was imposed with a fine of £18.4 million in 2018 for violating the security norms of data protection.

Ransomware attack on health service executive Ireland in March 2021: - The attacker succeeded because of easily targetable vulnerabilities and the network was less sophisticated. And the list is long.

PROBLEMS

Cyber attacks and advanced persistent threat lead to several problems in supply chain units like for instance loss of confidential and sensitive information that may further result in penalty imposition on vendors for compromising the sensitive information of their customers, numerous malware and BOT attacks that result in data corruption and breach of trustworthiness of SCM unit vendors and so on.

As per the reports of IntSight "Three Indian APT Groups"



HOW TO ALLEVIATE THE CYBER ATTACKS AND ADVANCED PERSISTENT THREAT

Asia-Pacific (APAC) Region's Chief Technology Officer Bryce Boland has reportedly said that though mostly organizations are seeking the legal security for advanced persistent threat(APT) solutions still relying solely on that is not sufficient for supply chain APT resilience. The APT and cyber attacks cannot be alleviated using single countermove but a sophisticated phenomena including people, processes, methodology and technology should be used. Suggested precautions to mitigate the APT attacks and to have resilience in SC units are technical diligence and surveillance, malware detection and eradication, containment of vulnerabilities and segregation of threatened components from whole network/software, data monitoring and network surveillance to identify double dealings, scrutinization of malware infiltration, technical up-gradation and advancement, prevention from backdoor penetration, use of software like Firewalls and network detection & response, training and technical up-gradation of IT/ Network personnel.

'Visibility' with respect to Supply chain

The translucency of trailing a product from the shipping initiation to the end delivery point is termed as visibility in SCM. That allows all the interested parties involved in the movement of a product from X to Y, to access the same valid and factual information at any point of time, mainly regarding status of inventories.

The visibility efforts

The mostly used software to enhance the visibility, now a days, mainly by apparel retailers globally is Radio Frequency Identification Technology (RFID) that requires encoding of information before it becomes visible to the reader. Companies like Adidas, Macy's, Secret and also many pharmaceutical companies are using RFID technology for tracking their inventories in Supply Chains. Also the SCM units are much inclined towards the warehouse buying and vertical and horizontal integration which are the recently emerged tools to enhance visibility with reduced risk of APT attack in more sophisticated manner and to mitigate the vulnerabilities for having supply chain resilience.

It is likely that in the process of re-configuration of supply chain strategies, industries would seek to construct a vigorous stock as hedge against supply chain interruptions. Many organisations would like to shift some parts of their supply chain in India only.

CONCLUSION

To eradicate and mitigate the threats of advanced persistent attacks and cyber-attacks including malware infiltration and data breach and assassination, SCM units are now much focused on technical up-gradation and advancement in addition to providing training to their employees to deal with such issues, rather than relying on traditional methods with legal assistance. According to Computer Emergency Response Team (CERT) the

compounded annual growth rate (CAGR) of cyber security products will see a growth of 17 per cent in 2022. The existing expenditure of $ 58 million on cyber security will reach $ 810 million by 2022 i.e. a 16 per cent increase in its CAGR. For increasing visibility, despite increased cost vertical and horizontal integration and warehouse buying are now seen as a weapon against APT in SCM .That also serves the purpose of inventory independency and help in achieving the goal of much advanced, sophisticated, re-imagined, re-configured and re-assessed business processes for supply chain resilience, especially after COVID-19. MA

References

Journals:-

1. *Supply chain management during and post-COVID-19 pandemic: Mitigation strategies and practical lessons learned - Alok Raja, Abheek Anjan Mukherjeea, Ana Beatriz Lopes de Sousa Jabbourb, Samir K. Srivastavac.*
2. *A brave new world: Lessons from the COVID-19 pandemic for transitioning to sustainable supply and production - Joseph Sarkis, Maurie J. Cohen, Paul Dewick, Patrick Schröder.*
3. *Role of Visibility in Supply Chain Management Zulkaif Ahmed Saqib, Khubaib Ahmed Saqib and Jin Ou Submitted: February 18th, 2019 Reviewed: June 3rd, 2019 Published: July 31st, 2019*
4. *Risk, resilience, and rebalancing in global value chains August 6, 2020 | Report by Susan Lund, James Manyika, Jonathan Woetzel, Edward Barriball, Mekala Krishnan, Knut Alicke, Michael Birshan, Katy George, Sven Smit, Daniel Swan, and Kyle Hutzler. Risk, resilience, and rebalancing in global value chains*

Websites:-

1. *httpspages.checkpoint.comsecurity-checkup.htmlutm_term=cyber-hub%20*
2. *httpswww.checkpoint.comcyber-hubthreat-preventionwhat-is-a-supply-chain-attack*
3. *httpswww.ncbi.nlm.nih.govpmcarticlesPMC8014293*
4. *httpswww.thehindubusinessline.comopinioncovid-19-exposes-indian-industrys-supply-chain-vulnerabilitiesarticle31224928.ece*
5. *httpswww.weforum.orgagenda2022015-ways-the-covid-19-pandemic-has-changed-the-supply-chain*
6. *httpswww2.deloitte.comglobalenpagesriskcyber-strategic-riskarticlescovid-19-managing-supply-chain-risk-and-disruption.html*
7. *www.csoonline.comarticle3647530supply-chain-vulnerability-allows-attackers-to-manipulate-sap-transport-system.html*
8. *atos.netenblogsolarwinds-attack-are-you-ready-for-the-supply-chain-risk*
9. *httpshakin9.orghow-to-prevent-and-detect-apt-attacks*
10. *httpshbr.org202009global-supply-chains-in-a-post-pandemic-world*
11. *httpsolidsystemsllc.comadvanced-persistent-threat-protection*
12. *httpstimesofindia.indiatimes.combusinessindia-businessdata-breach-cost-rises-by-8-in-2-yrsarticleshow72571373.cms*
13. *httpswww.bankinfosecurity.asianew-apt-threats-target-india-se-asia-a-8502*
14. *httpswww.darkreading.comthreat-intelligenceindia-s-cybercrime-and-apt-operations-on-the-rise*
15. *httpswww.accenture.comus-eninsightsconsultingcoronavirus-supply-chain-disruption*
16. *httpswww.chrobinson.comen-usresourcesblogwhy-is-supply-chain-visibility-so-important*
17. *httpsblog.worldfavor.comwhat-is-supply-chain-visibility-and-how-to-achieve-it*

AT THE HELM

Our heartiest congratulations to CMA G Srinivasan, Member of the Institute who has taken over the charge as Director (Finance) in South Eastern Coalfields Ltd, Bilaspur on 12.08.2022.

He has wide experience of more than 35 years in Finance Discipline in Coal Mining Industry and has served in various capacities in WCL, SECL and CIL. During his tenure at Coal India and subsidiaries, he has worked at Mines, Areas, Subsidiary Corporate Offices and CIL Corporate Office. He has handled various assignments such as Corporate Treasury Management, Direct and Indirect Taxation Matters, Corporate Accounts, Cost and Budget, Sales Account and other finance functions. He played a vital role in GST Implementation in SECL. He took a lead role and ensured successful implementation of ERP/SAP FICO Module in WCL and in all the Six subsidiaries of CIL in the Second Phase of ERP/SAP implementation. He is a Commerce Graduate from Madras University and an Associate Member of the Institute of Cost Accountants of India.

We wish CMA G Srinivasan the very best for all his future endeavours.