Impact Factor 6.1

Journal of Cyber Security

ISSN:2096-1146

Scopus

DOI

Google Scholar

More Information
www.journalcybersecurity.com

Crossref doi Google Scholar scopus

CYBER SECURITY IN SUPPLIER NETWORK IN SUPPLY CHAIN:

NAME: PALLIKKARA VISWANATHAN:

FACULTY: INDIAN INSTITUTE OF MATERIALS MANAGEMENT:

HOSUR BRANCH:

TITLE: Concept of Cyber Security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information on security. The term applies in a variety of contexts, from business to mobile computing, also can be divided into a few common categories of procurement, sourcing, warehousing operations, distribution, delivery in supply chain.

FIG 1_ CYBER SECURITY LOCK:

1. ABSTRACT OF THE STUDY/REVIEW:

Cyber security is the protection of internet-connected systems such as hardware, software and data from cyber threats. The practice is used by individuals, also by enterprises to protect

against unauthorized access to data centres also with other computerized systems in supply chain.

Cyber security is considered as a set of practices that is liable to protect the information systems of the suppliers", manufacturers, distributors, wholesalers, involved in supply chain, having the entire affect on the network, having network collaboration in supply chain.

Relationship with suppliers is to develop, a strong flow of information system, during Cyber Security adopted systems, audits, from suppliers, improvement of practices, encryption access, continuous intrusion detection systems, monitor vendor access network in supply chain.

Relationship with vendors, suppliers' training employees, on Cyber security risk, establishing security standards, protect protocols automations, reduce human errors, to an extended possibility, protecting interconnected network involved in the distribution of goods, does become an important activity in supply chain.

On the Intellectual Property Protection where sourcing, planning, scheduling execution controlling, monitoring flow of goods, services information with the concept of integration, needs protection of Cyber Security, on the various Cyber crimes promulgated in supply chain:

Key Words: Cyber Security: suppliers: manufactures: distributors: Network: relationship: Monitoring flow: Integration:

2. INTRODUCTION/PURPOSE/OBJECTIVE OF THE STUDY:

Introduction: Identifying risk management within Cyber security refers to the process that the technology is associated with the life-cycle on securing configuration, changes in management, penetration, testing in supply chain.

A list of leaked E-mail, address, names, Purchase, distribution, Phones numbers, insurance information, partial payment information, order delivery dates in supplier's network are to be coordinated among the process of Cyber Security process in supply chain.

Purpose: Digitalisation in business, Cyber attacks do frequently occur frequently in procurement, sourcing, planning, distribution, warehouse operations, as this enhanced Cyber Security, measures so as to protect supplier's, as this has the liability no exploit supplier's network in supply chain.

Cyberspace, often used interchangeably with the internet, is a complex and interconnected digital environment that doesn't have a physical presence but is built upon various technologies and components. The architecture of cyberspace is multifaceted and includes several key element, increase in operational efficiency, including network, data, social interactive in supply chain.

Study: E-Security in supply chain is the physical security system deployed, to bring in integration, facilitations, on the level of protection, on the physical access on the control

system of video surveillance system in supply chain in warehouse operation, known as Cyber Security, protecting the on-line system, also the network, devices operating in the warehouse systems or Stores, on the devices that are bound towards threats, tracking, data systems on order, materials, comprising of alarms access to controls of CCTV's in case of theft, misappropriation, in supply chain.

Objective: Encryption on hacker causing collateral damages on the accessing organisation software services, is liable to harm, also harm other multiple targets in supply chain, as this relies on the trust, among the service of customer, suppliers, sub-contractors, with Cyber Security in service in supply chain, with abilities to protect so as to comprise cash flow, payments systems, between the multiple organisation to gain access to sensitive financial information, disruption, theft, on Cyber Attack, gaining on operation, financial loss, damages, trust, also on the brand disruption in supply chain.

FIG 2_ **CYBER SECURITY LOCKING SYSTEM:**

3. PURPOSE OF THE STUDY:

Purpose: Network Infrastructure: This forms the backbone of cyberspace and consists of a vast, global network of interconnected devices and servers. This infrastructure includes the physical cables, routers, switches, and data centres that enable the transmission of data.

Integration becomes a primary concern in supply chain, on increasing leverage in Cyber Security, impersonation on supplier's identity, network, despite the risk, disruption involved with supplier's network, during transportation, delivery, operational involvement, as they

have fewer resources, limited capabilities, also make aware of the efficiencies, measures, speed, and cost on the related matters, that are likely to emerge in supply chain.

Study: Essential limited roles in securing Cyber Security is the integration with selection of supplier's, needs continuous development, having the knowledge of Cyber Security, as the supplier's become digitally connected in supply chain, likely to involve risk on environmental conditions, risk disruption regardless to the type of measures attributed in supply chain.

E-locking is a device of operation by means operations by electric current on external voltage, along with electronic control assembly with a lock mounted, using solenoid, electronic motor as an E-Security measure, in warehouses, Stores, suppliers, distributors, which is considered as measure of safety, secure, available on a E-locking electronic, Wi-Fi, capable to access the control system remotely locking, unlocking with the system monitoring, whether they are locked on a system in supply chain.

Conducted Study: In order to reduce risk in supply chain Cyber Security, continuous development of supplier, not as a single supplier, but multiple supplier's, is necessary to be integrated in a network, on the selection process, giving increasing knowledge on the technological development on Cyber Attacks in supply chain.

Prioritisation on the systems in supply chain, against damages, breaches, disruption risks, liable to destroy operations, on vulnerable conditions, in supply chain, cannot be sometimes be controlled, leading to unwanted predictable cost, inefficient delivery, intellectual property defamation, as this has to be comprised by Cyber Security, management, so as to enable to be not harmful to customer's, consumer's, bringing in better hope to the activities in supply chain.

4. LITERATURE REVIEW:

Development of software on products, on a single supplier network system, as the organisation become embedded on the various challenges, than that those that are conventional in supply chain, as they to rely upon the vulnerability 80% of the software, components in supply chain, this constitutes on how supply chain adheres to different software, availability over a time, as these challenges does exploit Cyber Attack on the Cyber Security systems in supply chain.

Bill of Materials is liable to have the detailed software systems for the 75% of the products, availability in quantity, specification, description of the item, requirements, also have the capability of tracking, on the emerging issues in production, manufacturing, as the software is liable to have the best Cyber Security systems to be adopted, so as to not manipulate, decipher the quantity in supply chain.

Communication and web technology have significantly transformed the way individuals and businesses interact, with Cyber Security, also operate in the digital age, that have some of the very key important points regarding the impact of the advancement on 60% in supply chain.:

Study: Legal signature in Cyber Security that becomes applicable on 75% of the documents generated for issues, requisitions, electronically in warehouse, ordering. E-mails, becomes an introduction concept, in the needed areas, of where Electronic Customer Relationship in management, for legal position dealing with electronically digital signature on product selection, vendor development, sub-contractors, as they do become business model, applicable to become electronically recognised in supply chain.

5. RESEARCH METHODOLOGY: PRIMARY/SECONDARY:

Primary; Researched: Global Connectivity: Web technology has enabled instantaneous communication in Cyber Security, also on the connectivity across the globe, facilitating real-time interactions between people, businesses, and governments, transcending geographical barriers in supply chain.

Web Security: The increasing complexity of web technology has also brought about concerns related to Cyber security, leading to the development of sophisticated security measures, also on various protocols to protect sensitive data, in order to ensure online safety in supply chain.

E-commerce: The proliferation of e-commerce platforms has transformed the way businesses operate, enabling online transactions, virtual storefronts, with global market access, leading to the rise of a digital marketplace in Cyber Security in supply chain.

Secondary: Researched: Cloud Computing: This technology has redefined data storage, also access, allowing businesses, also individuals to store, manage, have access to data, also with applications remotely connected over the internet, fostering enhanced collaboration, having accessibility, to the solution in Cyber Security service providers in supply chain. .

Mobile Technology: With the advancement of mobile devices, on better applications, adopted communication system , have become more portable, with convenience, enabling users to access the internet, communicate, also to enable to conduct business on the various goings of maintaining Cyber Security in supply chain..

6. RESULTS:

Real-Time Communication Tools: Various real-time communication tools such as video conferencing, instant messaging, and VoIP (Voice over Internet Protocol) have facilitated seamless communication between individuals, also businesses organisations, enhancing productivity, with better collaboration in supply chain.

Internet of Things (IoT): The Internet of Things have further expanded the capabilities of web technology, enabling the interconnection of various devices, also on the various complicated systems, leading to the creation of smart homes, cities, also different types industries, thereby enhancing efficiency, better convenience, on transportation of raw materials, reversal logistics, as applied to Cyber Security in supply chain.

Artificial Intelligence (AI) Integration: Artificial Intelligence have been integrated into communication, also into Web technology, enabling personalized user experiences, predictive analytics, with better automation, thereby streamlining processes, also bringing in improvement in decision-making also on the change management in supply chain.

Social Media: Platforms such as Face book, Twitter, Instagram, also LinkedIn have revolutionized communication, in Cyber Security, allowing users to share information, connect with others, also engage in various forms of online collaboration with knowledge management in supply chain.

Risks in supply chain includes incorporation of counterfeit, unauthorised manufacturing, theft, software, hardware insertion, on a responsibility to protect Cyber Crimes within the organisation, on standard practices attained, can give preference to Cyber Security, on the combination of risks, disruption, focussing on inventory control visibility, with the help of globalisation, outlined with predictive analytic in supply chain.

Result: Predictive analytics in supply chain Cyber Security network in a supplier is a process through which efficient, effective strategies on planning, results in improvement in procurement, sourcing, inventory control, distribution, transportation, delivery (includes last mile delivery) system, is to be improved through optimised procedure, having increased knowledge management, in order to increase profitability, by proper planning on the technology, under the pressure of Generative AI on artificial intelligence, machine learning, Gen GPT, Next, using the best sophisticated model, (penetration, Firewalls) also with the help of algorithms'(a procedure to encrypt data) towards effective, efficient implementation, so as to bring improvement on threats so as to bridge the business development in supply chain.

7. DISCUSSIONS AND FINDINGS:

Discussions: Block chain Technology: Block Chain have been introduced to be secure, also on a transparent methods for conducting online transactions, thus for maintaining digital records, that is likely to have impact on various industries, including finance, management, also on the healthcare. Cyber Security adopted systems in supply chain.

Understanding the impact of communication and web technology is crucial for businesses and individuals alike, as it facilitates effective communication, enhances productivity, and fosters innovation in various domains. However, it is essential to remain aware of the potential challenges and risks associated with these advancements, particularly in terms of privacy, security, and ethical considerations.

Findings: Implementation of Cyber Security controls, protection of the required data, that have been classified, as confidential, is to be ensured that vendors, suppliers, sub-contractors, are very much compliant with the regulatory local governing laws, as well as data protection laws, as that become applicable for services rendered under the contract in supply chain.

Disruption of supply chain that goes beyond any Cyber attack, becomes rather vulnerable in supply chain, Cyber Security should be enabled to find the reason for the cause, which is likely to cause disruption, risk problems, to transportation system, manufacturing facilities, as this is likely to cause delays, disruption in financial delays, cascading the affect in supply chain.

8. FUTURE WORK/CONCLUSIONS/RECOMMENDATIONS:

- **Future Work**: Network Cyber Security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware. Application Cyber Security focuses on keeping software, with devices free from threats in supply chain..

  Compromised application could provide access to the data, as it is designed to protect, successful Cyber Security as it begins in the design stage, well before a program or device is deployed in supply chain

- **Conclusions**: Information on Cyber Security protects the integrity, also the privacy of the data, both on storage, also in the transit, on the operational Cyber Security, which includes the processes, also on the decisions for handling, protecting the data on assets in supply chain, with the permissions of the users, have been when accessing the network, also among the procedures, that determine how also it becomes necessary to know where the data may be stored or shared, that is likely to fall under the umbrella of supply chain..

  Disaster recovery, with continuity in business defines, how an organization responds to a Cyber-Security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan that the organization falls back on while trying to operate without certain, or any resources in supply chain..

- **Recommendations:** End-user in education addresses the most unpredictable cyber-security factor: for the benefit of the people. Accident can happen in supply chain to anyone part that can accidentally introduce a virus to an otherwise secure Cyber Security system by failing to follow good security practices. Teaching, training methods adopted having been used to delete suspicious email attachments, not in able to plug in unidentified USB (flash drive or memory stick) drives, on the various important lessons, methods, that is vital for the Cyber Security in any organization in supply chain.

LIMITATIONS:

Issues and challenges of cyber security:

Cyber Security is a critical and ever-evolving field that faces numerous issues and challenges. As technology advances, so do the tactics and techniques of cybercriminals, try to make progress, then Cyber Security tightens in supply chain. Here are some of the key issues and challenges in the field of Cyber Security:

1. Rapidly Evolving Threat Landscape: Cyber threats are constantly evolving, becoming more sophisticated and harder to detect. New attack vectors, malware, and vulnerabilities are discovered regularly, making it challenging for organizations to keep up.

2. Advanced Persistent Threats (APTs): APTs are targeted, long-term Cyber attacks by well-funded and organized groups. They can go undetected for extended periods, making them a significant challenge for organizations in Cyber Security in supply chain.

3. Insider Threats: Malicious or negligent actions by employees, contractors, or business partners can pose a significant security risk in Cyber Security attack in supply chain. Organizations must address both intentional and unintentional insider threats, that become a part in supply chain..

4. Lack of Cyber Security Awareness: Many individuals and employees lack the awareness, also the knowledge to recognize, and prevent cyber threats, such as phishing attacks and social engineering persisted in supply chain..

5. Shortage of Skilled Professionals: There is a shortage of Cyber Security professionals with the necessary skills, and expertise to defend against cyber threats. This talent gap is becoming a growing concern for organizations in supply chain.

6. Resource Constraints: Smaller organizations may lack the financial constraints, also requirement of human resources required to establish and maintain effective Cyber Security measures, making them vulnerable to attacks in supply chain.

7. Complexity of IT Environments: Complex IT environments, with a mix of on-premises, and cloud-based systems, increase the cyber attack surface, and make it harder to secure all assets effectively in supply chain.

8. Mobile and Internet of Things Security: The proliferation of mobile devices and IoT (Internet of Things) devices introduces new security challenges, as these devices often lack robust Cyber Security features in supply chain.

9. Cloud Security: As more organizations move their data and operations to the cloud, ensuring the security of cloud-based services becomes crucial. Configured missed in cloud settings, need inadequate security controls can lead to data breaches in supply chain..

10. Data Privacy and Compliance: Regulations like General Data Protection Regular and Central Consumer Protection Authority require organizations to protect personal data and maintain compliance, since violations can result in severe fines, reputational damage in Cyber Security in supply chain. .

11. Ransomware (unauthorised attack that locks, encrypts, data of victims, systems, rendering them unaccessable) attack has become one of the a biggest attack, considered as the biggest threat on Cyber Security, in supply chain, on malicious codes, injected into the software updates, attacks on Information Technology, operational technology, exploitation vulnerable, including flow of assets, processing in packing, distribution in supply chain.

Limitations: Cyber Security insurance on Cyber liability (organisation to account for implementation on data breach) is a contact that helps to reduce the financial risk, if procurement is on-line, monitoring vendors, suppliers, access on to a network data, by training personnel, implementing controls, reviewing suppliers, trying to implement policies, procedures, to protect against internal, external conditions, using software Bill of materials, to understand the description of materials, specification, quantity, required for easy tracking, on the potential vulnerabilities in supply chain.

REFERENCES:

SOURCES OF INFORMATION FROM THE ELECTRONIC MEDIA:

1. **CYBER SECURITY IN SUPPLY CHAIN SECURING BUSINESS ECO SYSTEM neumetro publication**
2. **CYBER SECURITY IN SUPPLY CHAIN SCCG Publication in supply chain:**
3. **CYBER SECURITY FOR INDUSTRY NETWORK Security Xcekerator Siemans:**
4. **CYBER SECURITY A THIRD PARTY SUPPLIER RISK Author Nasir Ali CA CFE 1st April 2022:**