UNIT IV

TECHNICAL SECURITY

Supply Chain Management-Cloud Security

Supply chain security is the part of supply chain management that **focuses on the risk management of external suppliers, vendors, logistics and transportation**. Its goal is to identify, analyze and mitigate the risks inherent in working with other organizations as part of asupply chain.

The five different processes which are also known as components of

Supply ChainManagement – **Plan, Source, Make, Deliver and Return**.

The 6 Supply Chain Models

- The continuous flow models.
- The fast chain models.
- The efficient chain models.
- The custom configured model.
- The agile model.
- The flexible model.

The 2 Types of Supply Chains are

Reactive Supply Chain Strategy

Operational improvements based on guesswork or imitating competitors

Data-Driven Supply Chain strategy

A data-driven approach helps even best-in-class manufacturing operations find new ways to improve efficiency

How to Implement Cyber Security Strategies for Supply Chain:

The following four steps can help the company implement cyber security strategies to improve its supply chain risk management approach.

1. Fully understand the threat to the supply chain business.

This step requires the team to completely review, learn, and keep track of all supply chain breaches, data leaks, and malware attacks that affect the company.

Assess your cyber security measures: The cybersecurity team needs to know what measures are already in place and which are missing. This framework includes hardware used to prevent or mitigate incursions, software used on network computers, education, AI, and purchased tools.

2. Improve current measures. After understanding what you already have and assessing how these tools can assist with cybercriminal attacks, you can then improve these measures already in place.

Treat cyber security as an ongoing process. Once you learn how to best increase security within the business against security incidents, you will need to document, review, and sift through feedback.

Some ways to prevent a cyber attack include:

- Double-check emails for possible phishing attempts.
- Inform cyber security agents immediately if a threat is identified.
- Use tools all employees can access to prevent unauthorized access,breaches or data leaks.
- Educate your entire staff on best practices to avoid cyberattacks. They areyour first line of defense.
- Invest in protective tools that will guard against attacks.
- Work with cyber security experts to identify additional points of protection.
- Always use strong passwords and multi-factor authentication

CLOUD SECURITY:

Cloud security, also known as cloud computing security, consists of a set of policies, controls,procedures and technologies that work together to protect cloud-based systems, data, and infrastructure.

These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users anddevices.

From authenticating access to filtering traffic, cloud security can be configured to the exactneeds of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be responsibility between the business owner and solution provider.

Why is cloud security important?

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computingis no less at risk than an on-premise environment.

Cloud security offers many benefits, including:

Centralized security: Just as cloud computing centralizes applications and data, cloud securitycentralizes protection. Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with shadow IT or BYOD.

Managing these entities centrally enhances traffic analysis and web filtering, streamlines themonitoring of network events and results in fewer software and policy updates. Disaster recovery plans can also be implemented and auctioned easily when they are managed in oneplace.

Reduced costs: One of the benefits of utilizing cloud storage and security is that it eliminates theneed to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads.

Reduced Administration: When you choose a reputable cloud services provider or cloud security platform,. These tasks can have a massive drain on resources, but when you move themto the cloud, all security administration happens in one place and is fully managed on your behalf.

Reliability: Cloud computing services offers the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what devicethey are using.

Cloud computing allows organizations to operate at scale, reduce technology costs and use agilesystems that give them the competitive edge. However, organizations have complete confidencein their cloud computing security and that **all data, systems and applications are protected from data theft, leakage, corruption and deletion.**

Secure Data in the Cloud:

Cloud data security becomes increasingly important as we move our devices, datacenters, business processes, and more to the cloud.

Ensuring quality cloud data security is achieved through comprehensive securitypolicies, an organizational culture of security, and cloud security solutions.

Selecting the right cloud security solution for business is imperative the cloud and ensure yourorganization is protected from unauthorized access, data breaches and other threats.

Forcepoint Cloud Access Security Broker (CASB) is a complete cloud security solution that protects cloud apps and cloud data, prevents compromised accounts and allows you to set security policies on a per-device basis.