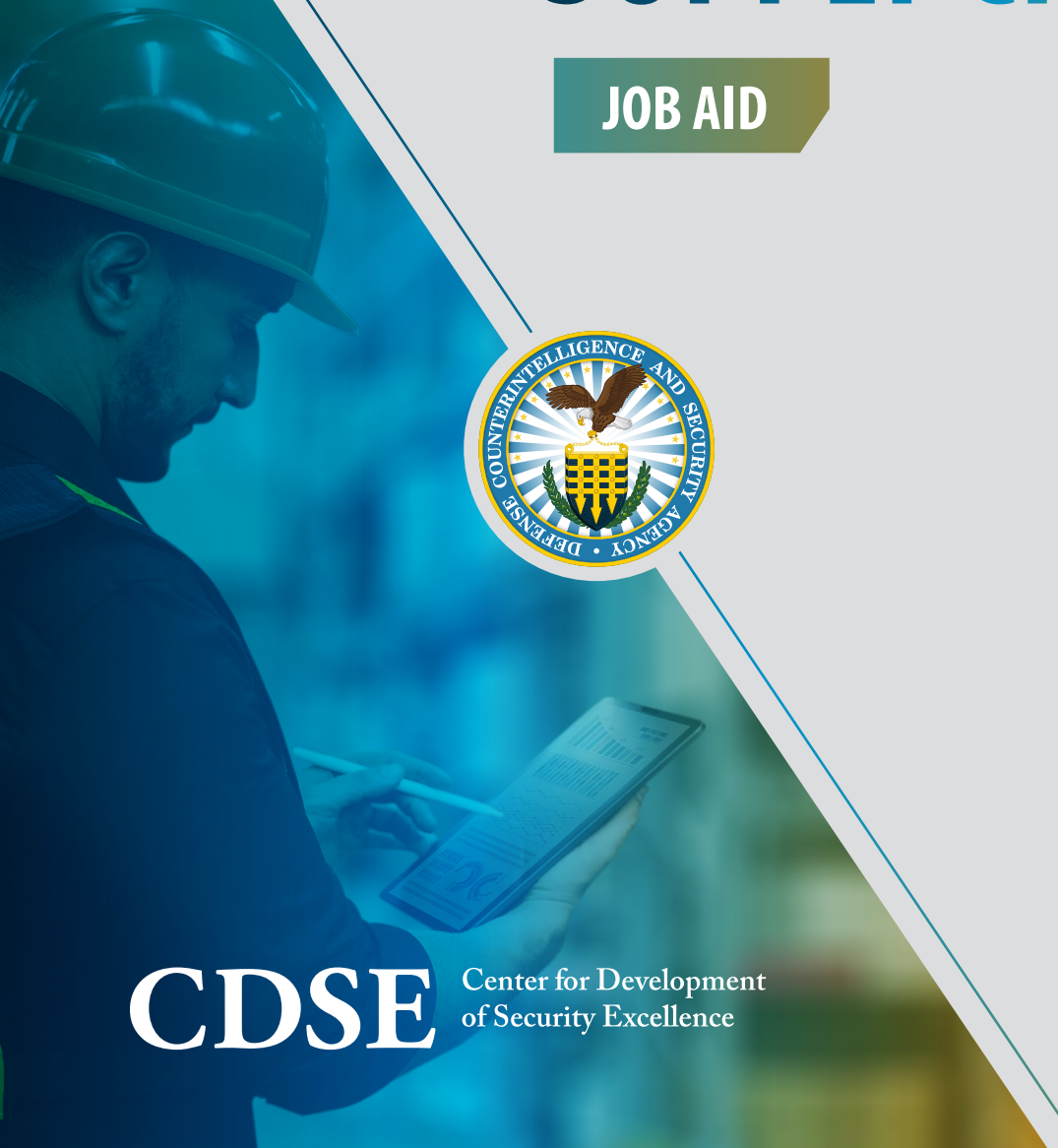
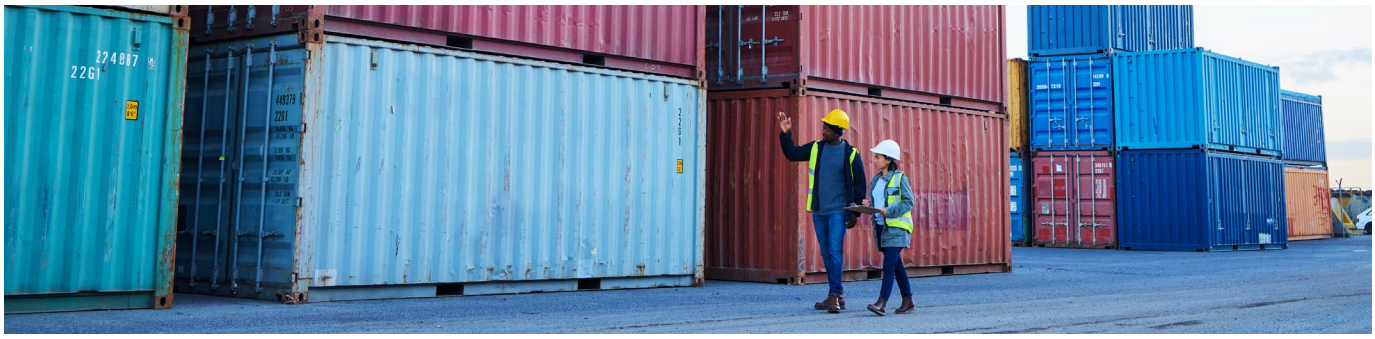
December
2024

INSIDER THREAT TO SUPPLY CHAINS

JOB AID



CDSE Center for Development of Security Excellence



INTRODUCTION

What Is a Supply Chain Insider Threat?

Supply chain security is a crucial component of any organization that deals with the movement of goods and services. It involves ensuring products are not tampered with or stolen during the production, storage, transportation, or delivery process. However, what many companies overlook is the risk posed by internal sources – insider threats.

An insider threat in the context of supply chain security is a risk to an organization's goods, services, or data that comes from an individual within the organization who has authorized access to them. This could be a current or former employee, a contractor, or anyone with access to sensitive information or systems. Insider threats can cause significant damage to a company's reputation, finances, and competitive advantage.

Internal risks may not always be malicious, as they can also be caused by employees unintentionally exposing confidential information, making mistakes, or disregarding protocols. Nonetheless, the damage can be severe, which is why organizations need to be proactive in identifying and mitigating the risks.

The first step to preventing insider threats in supply chain security is to understand the different types and how they can occur.

Common Supply Chain Insider Threat Examples

- **EMPLOYEE MISUSE:** One of the most common forms of insider threats is employee misuse of systems or data. This can include employees intentionally sharing or leaking sensitive data, using company resources for personal gain, or engaging in unauthorized activities.
- **THIRD-PARTY CONTRACTORS:** Third-party contractors often have access to sensitive data and systems. A contractor with malicious intent could use their access to steal sensitive data or launch a cyberattack.
- **COMPROMISED ACCOUNTS:** An insider threat could also come from a compromised account. Cybercriminals may gain access to an employee's login credentials, allowing them to impersonate that employee and gain access to sensitive data.
- **SABOTAGE:** Another potential insider threat is sabotage. An employee could intentionally delete important data, alter critical systems, or damage equipment.

By understanding the different types of insider threats, you can better identify potential risks and vulnerabilities in your supply chain. It is important to implement best practices for preventing insider threats, such as regularly reviewing access privileges and monitoring system activity for suspicious behavior.

LEARN MORE: Effective Supply Chain Risk Management (SCRM) can mitigate these risks and ensure DOD technology is delivered uncompromised. Learn how through the Defense Acquisition University course Supply Chain Risk Management for Information and Communications Technology (CLE080).

EXAMPLES OF SUPPLY CHAIN INSIDER THREATS

December 13, 2020: Hackers Targeted SolarWinds

SolarWinds was a third-party compromise that affected more than 18,000 SolarWinds customers who installed the malicious updates. Through this code, Russian hackers accessed SolarWinds's customer information systems, which they could then use to install even more malware to spy on other companies and organizations.

"Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations" | CISA Cybersecurity Advisory

October 24, 2022: U.S. Superconductor Company Targeted for Trade Secrets

Through a use of employee misuse and contract abuse, a U.S. company engaged in a business relationship with a Chinese wind turbine manufacturer and became the victim of conspiracy to commit trade secret theft, theft of trade secrets, and wire fraud. After signing over $800 million in contracts with the U.S. company, the Chinese company severed its relationship and recruited an insider from the U.S. company to provide intellectual property to the Chinese company.

"A U.S. Superconductor Company Targeted for Trade Secrets" | Federal Bureau of Investigation

May 16, 2024: IT Workers Infiltrated More than 300 U.S. Companies, Earning Millions

Nefarious foreign agents supporting the North Korean government used compromised accounts and credentials to conduct employee misuse, sabotage, and intellectual theft of over 300 companies that hired North Korean Democratic People's Republic of Korea (DPRK) IT workers who used stolen or borrowed U.S. person identities to raise hard currency revenue for the DPRK. The scheme ran from at least October 2020 through October 2023.

"Charges and Seizures Brought in Fraud Scheme Aimed at Denying Revenue for Workers Associated with North Korea" | United States Department of Justice

LEARN MORE: Readers should further consult applicable and controlling laws, regulations, policies, and procedures. Visit CDSE for additional training and resources.

MITIGATING SUPPLY CHAIN INSIDER THREATS

Understanding Supply Chain Security Principles

- Develop your defenses based on the principle that your systems *will* be breached.
- Cybersecurity is never just a technology problem; it's a people, processes, and knowledge problem.
- There should be no gap between physical and cybersecurity.

Mitigating supply chain insider threats can help prevent damage to operations, safety, compliance, reputation, and trust.

- Identifying and understanding the risks and vulnerabilities. Conduct regular security audits and vulnerability assessments of your supply chain to identify potential areas of weakness. Analyze the risk posed by employees, contractors, and third-party vendors with access to sensitive data or critical assets.
- Utilize robust security protocols, such as zero trust architecture, data encryption, limiting access control, and identity management systems. Provide regular training on security policies, procedures, and expectations.
- Monitor and conduct regular audits to assess accesses to critical systems, data, and assets to detect and determine if unauthorized access has been made or to identify any malicious activities.
- Develop and establish a response plan for security incidents. Establish an incident response team with clear roles and responsibilities.
- Provide regular security awareness trainings and include insider threat scenarios in tabletop exercises to help employees understand the importance of Supply chain security and how to detect and report suspicious activities.

Identifying Potential Risks and Vulnerabilities:

- **CONDUCT A RISK ASSESSMENT:** Start by conducting a risk assessment to identify potential vulnerabilities in your supply chain. This assessment should include a review of your existing security measures, processes, and policies, as well as an analysis of the threats facing your organization.
- **MONITOR EMPLOYEE BEHAVIOR:** Monitoring employee behavior through activity logs, network traffic analysis, and other methods can help you identify potential risks before they become security incidents.
- **LIMIT ACCESS:** Access controls should be based on the principle of least privilege, which means granting employees only the minimum level of access required to perform their job functions.
- **ESTABLISH STRONG AUTHENTICATION AND AUTHORIZATION PROCEDURES:** This includes requiring strong passwords, multi-factor authentication, and regular password changes.

You can reduce the likelihood of insider threat incidents in your supply chain by taking steps to identify potential risks and vulnerabilities. However, it's important to recognize that no security measure is fool proof, and it's critical to have a plan in place for responding to insider threats when they occur.

LEARN MORE: Take the Supply Chain Risk Management Self-Assessment Tool and Checklist.

BEST PRACTICES FOR PREVENTING SUPPLY CHAIN INSIDER THREATS

When it comes to preventing insider threats in the supply chain, there are several best practices that organizations can follow to protect their sensitive data and operations. Here are a few tips:

- **DEVELOP A STRONG SECURITY CULTURE:** Developing a culture of security is essential to preventing insider threats. This means providing regular security awareness training, monitoring employee behaviors, and enforcing security policies and procedures.
- **COMPREHENSIVE RISK ASSESSMENTS:** Conduct regular assessments of all vendors and third-party service providers.
- **CONDUCT BACKGROUND CHECKS:** Before hiring any new employees, it's important to conduct thorough background checks to ensure they have a clean record and no previous history of malicious activities.
- **USE LEAST PRIVILEGE:** Limiting access to sensitive data and systems to only those employees who need it is another way to prevent insider threats. This practice is known as least privilege.
- **CONTINUOUS MONITORING:** Keep a close eye on employee behavior and monitor their access to sensitive data and systems. This can help detect any abnormal or suspicious activity early on.
- **CREATE A STRONG INCIDENT RESPONSE PLAN:** Having a well-designed incident response plan is critical to responding quickly and effectively to any potential insider threats.
- **INFORMATION SHARING:** Collaboration and information sharing between private and public sectors can enhance the ability to detect and respond to sophisticated cyber threats.
- **THIRD-PARTY RISK MANAGEMENT:** Vendors and contractors should adhere to the same security standards as the contracting company itself.

By implementing these best practices, organizations can take proactive steps to prevent insider threats and minimize the risks associated with the supply chain security. Remember, it only takes one bad actor to cause serious harm to your operations.

ADDITIONAL RESOURCES

Center for Development of Security Excellence (CDSE)

Cyber Insider Threat (eLearning Course)

Cybersecurity Attacks: The Insider Threat (Short)

Counterintelligence Awareness/Supply Chain Risk Management Toolkit

Potential Risk Indicators: Insider Threat (Job Aid)

Twitter Smartcard

An Alternative View of Preventing Insider Threats: Taking Culture Seriously (Webinar)

Cybersecurity Toolkit: Supply Chain Risk Management

National Counterintelligence and Security Center (NCSC)

Supply Chain Threats

Cybersecurity and Infrastructure Security Agency (CISA)

Supply Chain Integrity Month

Insider Threat Mitigation Resources and Tools

Information and Communications Technology Supply Chain Security

U.S. Department of Commerce

Insider Risk Management Program Office

National Institute of Standards and Technology

Best Practices in Cyber Supply Chain Risk Management

NOTE: If the URLs in this document do not open upon clicking, right-click on the hyperlinked text, copy link location, and paste into a browser. Alternatively, you can open the PDF in a browser.