Issue Tree Analysis: Cybersecurity and Supply Chain Threat Landscape

Adam Mohmoud

Georgetown University

BLVH 2302: Global Competitive Intelligence

Dr. Shadi Abouzeid

November 10, 2024

Brief 1: You work at the DC Fusion Center. Your line manager is worried about the increasing Cybersecurity threats originating from adversarial countries.

Issue Statement: How can the DC Fusion Center proactively enhance its cybersecurity posture to effectively mitigate the evolving threat landscape and frequency of attacks posed by adversarial countries, while optimizing resource allocation and fostering collaboration across key stakeholders?

To effectively address this multifaceted issue, the initial approach would be to utilize the "Hypothesis Tree." The Hypothesis Tree will facilitate a deep dive into the root causes of vulnerability to attacks by adversarial countries, allowing for a structured analysis of the threat landscape and potential points of failure, including technological limitations, operational gaps, and intelligence shortcomings. In the subsequent phase, the Solution Tree will be utilized to enable the identification and evaluation of potential solutions, empowering innovative thinking and data-driven decision-making while documenting viable mitigation strategies.

Hypothesis Tree:

Key Issue	Sub-Issue Level 1	Sub-Issue Level 2	Sub-Issue Level 3
Why is there an increase in cybersecurity threats from adversarial countries?	Threat Landscape	Attack Mechanisms	a. Malware attacks are designed to gain unauthorized access, steal data, and disrupt systems b. Phishing Scams are deceptive attempts (e.g. via email) to reveal financial information or organization credentials c. Denial of Service (DOS) attacks flood a system with traffic to prevent legitimate users from access
		Frequency	a. Increasing complexity of attack techniques making detection and prevention more challenging b. Rising rate of attacks increase the likelihood of successful system/data breaches
		Targeting	a. Critical infrastructures are especially vulnerable to attack b. Government Networks often have weak security practices and outdated systems increasing their vulnerability to attack c. Private sector is vulnerable to data breaches as an attacker's goal is to gain a competitive advantage or cause economic harm
	Vulnerabilities	Critical Infrastructure	a. Legacy Systems often rely on outdated technology which makes It more vulnerable to attack b. Interdependent/interconnected networks make systems more vulnerable from upstream failures of a compromised system or application c. Lack of security updates and patches leave the system or application open to vulnerabilities
		Government Networks	a. Inadequate security protocols often have weak security practices and outdated systems b. Malicious threats from insiders are especially harmful to government systems and applications c. Lack of security training for employees make them more susceptible to phishing and other social engineering attacks

		Private Sector Networks	a. Insufficient security awareness training for their employees due to lack of resources, education, and funding b. Weak or outdated access controls, passwords, lack of multi-factor authentication allow access c. Poor incident response planning to a cyberattack negatively impact the system and organization
	Adversarial Capabilities	Motivation & Goals	a. Economic gain from cyber theft and/or disrupting financial markets b. Political gain by influencing elections, spreading disinformation, or disrupting government operations c. Military gain by stealing military technology, disrupting military operations, and gaining a strategic advantage
		Resources & Tools	a. Cybercrime groups from countries that harbor and support them by providing them resources to commit cybercrime b. State-Sponsored groups are well-funded and have access to sophisticated tools and advanced techniques
		Espionage & Data Breaches	a. Intelligence gathering to steal sensitive information (e.g. classified documents, intellectual property, personal data) from government, military, and private organizations. b. Sabotage used to disrupt critical infrastructure, cause economic disruption, cause chaos, or a prelude to military action c. Data Theft includes stealing sensitive data for nefarious purposes (e.g., financial gain, identity theft, or blackmail)

Brief 2: You are a member of the strategy team at a multinational organization. Different departments are suffering from delays in production and customer service delivery due to issues in the supply chain.

To address supply chain issues affecting multiple business areas, using a problem or "why" tree is essential for identifying root causes. Workforce indicators such as labor shortages and company reorganizations can contribute to operational risks. Outdated technology and systems can limit operational outputs and inefficiently streamline data across the chain of operations and other departments. Additionally, systems that aren't patched or updated efficiently are susceptible to cyber threats. A lack of supplier diversity can jeopardize production output, failing to meet demand. Strengthening product sources with various suppliers and implementing an optimal system to respond to market shifts during recessions and inflation is critical. A diverse portfolio globally can help an organization's supply chain function effectively during times of geopolitical instability and political climate changes that influence policy. Implementing these mitigation strategies is crucial for creating an optimal supply chain to support various business areas.

Key Issue	Sub-Issue Level 1	Sub-Issue Level 2	Sub-Issue Level 3
What is happening in our supply chain that is causing issues with several departments?	Workforce	Labor shortages	Labor shortages can cause delays resulting in both increased costs and dissatisfied customers.
		Internal issues	Company reorganizations and implementing new business strategies that can impact supply chain management, supplier relationships, and create insufficient visibility.
		Operation risks	Poor workforce training can lead to insufficient processes, management tactics, and quality problems.
	Technology and systems	Outdated systems	Old systems that cannot integrate with ERP software can limit scalability.
		Cybersecurity vulnerabilities	As a result of labor shortages, a lack of expertise and insufficient tools to perform vulnerability checks, system audits, and assess cybersecurity posture.
		Data miscommunication	Failure to transition to digital transformation to automate data collection and using IoT devices to create a more efficient supply chain.
	Product Sources	Lack of diverse suppliers	Diversifying suppliers to maximize the efficiency of supply chain operations. If one supplier has issues another can fill demand.
		Geopolitical risk	Political climate shifts and instability where supply chains operations and suppliers are active can cause severe supply chain disruptions.
		Economic risk	Lack of a flexible framework to adapt to market shifts in demand, inflation, and recessions can have impact on availability.

Reference Page

Abouzeid, S. (2024). *Issue Statements/Issue Trees* [Video]. Coursera, 31 October 2024, https://www.coursera.org/learn/global-competitive-intelligence/lecture/ApsXF/abouzeid-s-2024-issue-statements-issue-trees

Cimcor Security Guide: System Hardening Checklist for Systems/Devices (2022). International Trade Administration, 4 November 2024, https://www.trade.gov/sites/default/files/2022-10/Cimcor%20Security%20Guide%20-%20System%20Hardening%20Checklist%20v2.pdf

CISA Resources & Tools (N.d.). Cybersecurity & Infrastructure Security Agency, 4 November 2024, https://www.cisa.gov/resources-tools/services

The Definitive Guide to Issue Trees (N.d.). Crafting Cases, 31 October 2024, https://www.craftingcases.com/issue-tree-guide/

Witcher, R. (2024) *CISSP Common Body of Knowledge (CBK): The 8 Domains Explained*. Destination Certification, 31 October 2024, https://destcert.com/resources/8-cissp-domains-explained/