70 AÑOS

FCE Facultad de Ciencias Económicas

AEO from a cross border perspective: a proposal for risk management in digital supply chains

Sebastián Galindo Cantor

Gloria Rodríguez Lozano PhD., MSc.

Escuela de Administración y Contaduría Pública
Sede Bogotá

FCE Facultad de Ciencias Económicas

UNIVERSIDAD NACIONAL DE COLOMBIA

70 AÑOS

FCE Facultad de Ciencias Económicas

"(…) We should treat personal electronic data with the same care and respect as weapons-grade plutonium – it is dangerous, long-lasting and once it has leaked there's no getting it back. (…)"

Cory Doctorow.

Index

1. General Context on Digital Supply Chain and Risk management.

2. Proposal from the AEO perspective.

3. Conclusions and recommendations.

1. General Context on Digital Supply Chain and Risk management

New concept on Supply Chain

e-commerce

Digitalization

Interconnectivity- interoperability

1. General Context on Digital Supply Chain and Risk management

18,000 of their clients downloaded an affected version.

US government institutions and agencies such as the Department of Homeland Security, the State Department, the National Nuclear Security Administration

Cisco, Intel, Deloitte and Microsoft as some medical institutions and hospitals

invima
Instituto Nacional de Vigilancia de Medicamentos y Alimentos.

Source : 2021 Software Supply Chain Security Report – Argon 2021

1. General Context on Digital Supply Chain and Risk management

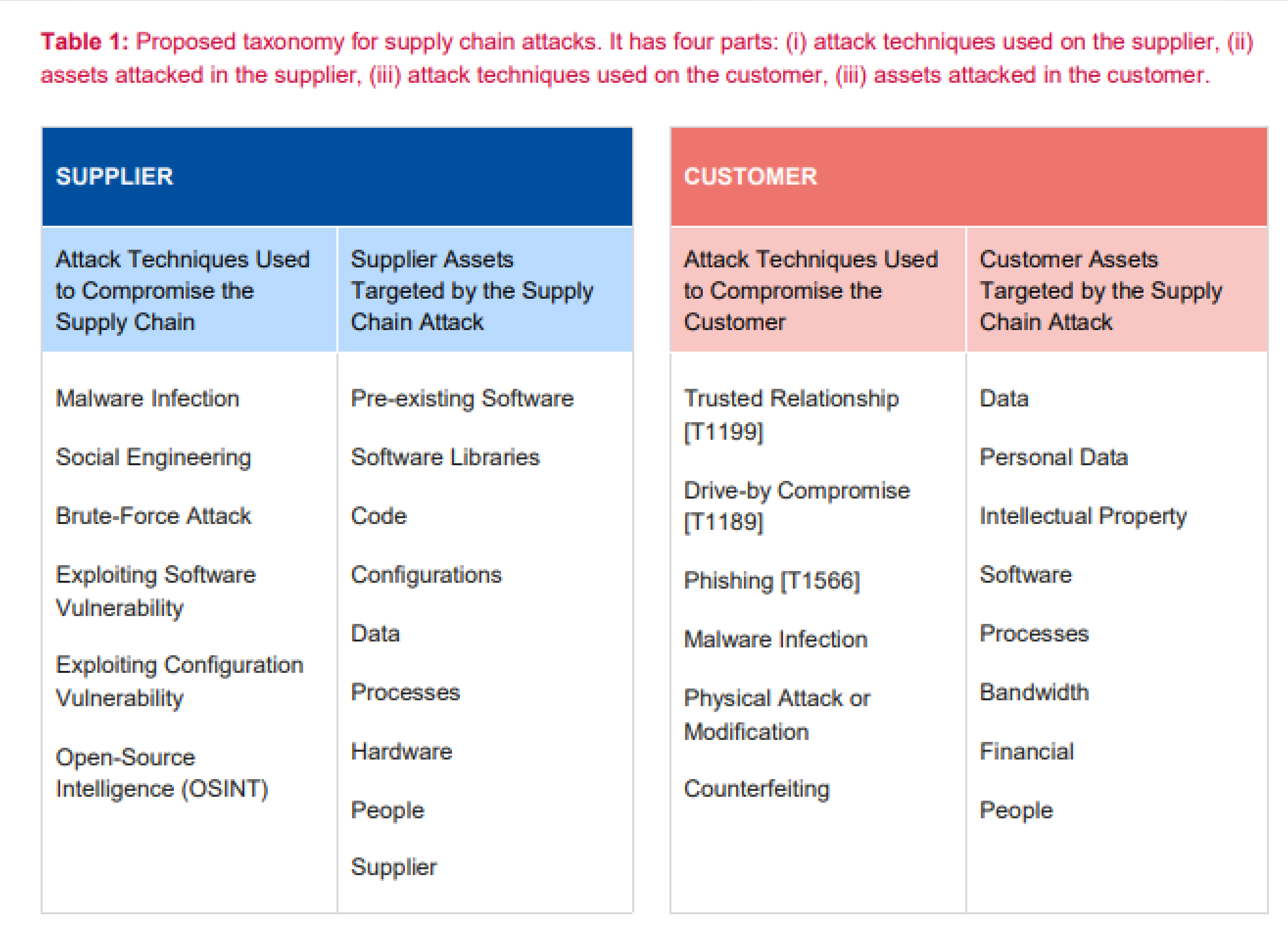
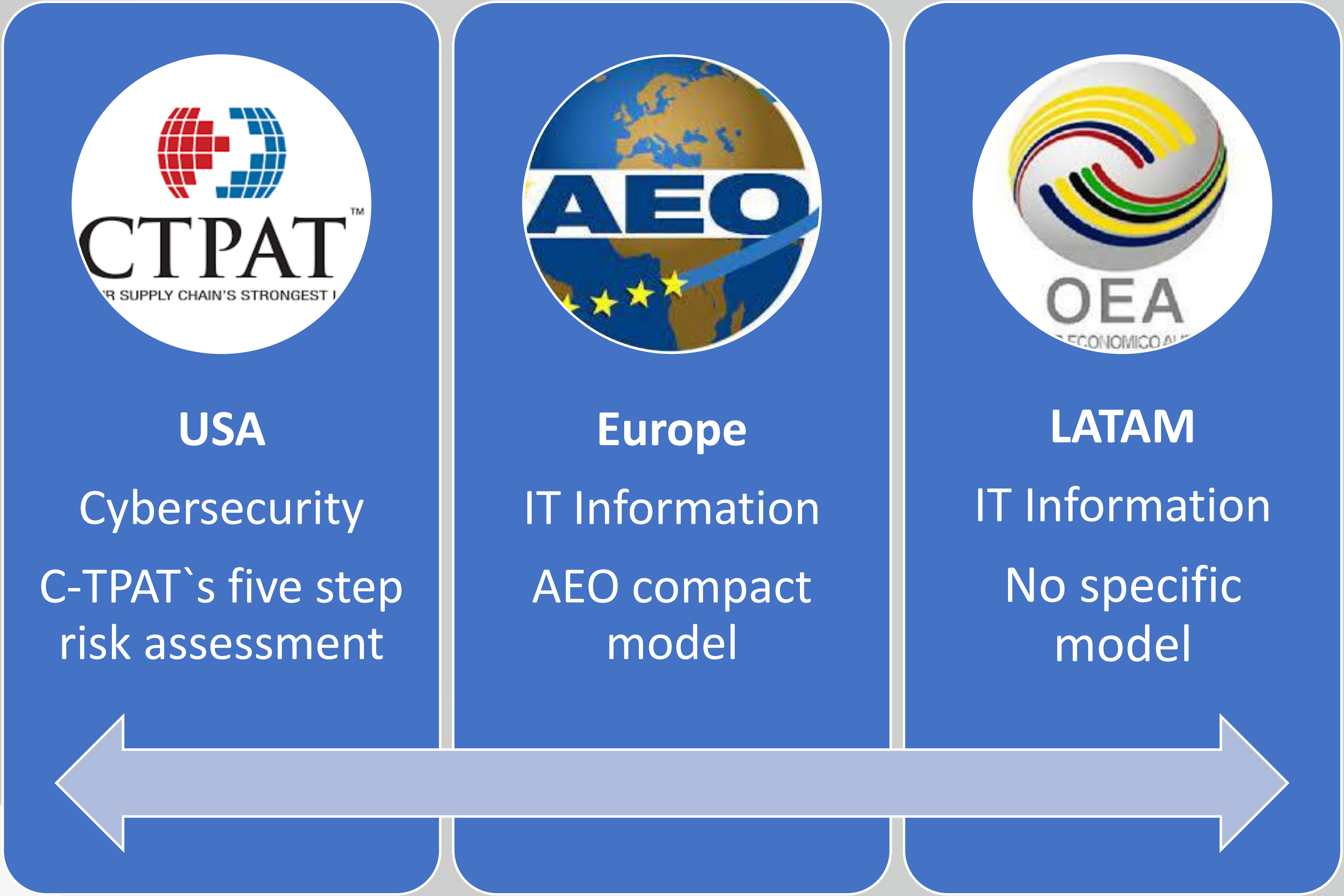


Table 1: Proposed taxonomy for supply chain attacks. It has four parts: (i) attack techniques used on the supplier, (ii) assets attacked in the supplier, (iii) attack techniques used on the customer, (iii) assets attacked in the customer.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection Social Engineering Brute-Force Attack Exploiting Software Vulnerability Exploiting Configuration Vulnerability Open-Source Intelligence (OSINT)	Pre-existing Software Software Libraries Code Configurations Data Processes Hardware People Supplier	Trusted Relationship [T1199] Drive-by Compromise [T1189] Phishing [T1566] Malware Infection Physical Attack or Modification Counterfeiting	Data Personal Data Intellectual Property Software Processes Bandwidth Financial People

Source : European Union Agency for Cybersecurity . (2021)

1. General Context on Digital Supply Chain and Risk management



USA

Cybersecurity

C-TPAT`s five step risk assessment

Europe

IT Information

AEO compact model

LATAM

IT Information

No specific model

Source: European Commission Taxation and Customs Union 2015; U.S Customs and Border Protection 2021 ; ALADI 2020

Four key elements can be established within the context of risk management for AEOs:

1. Supplier: is an individual, individuals, groups of individuals, or organizations that supply a product or service to another individual, individuals, groups of individuals, or organizations that are called a customer.

2. **Supplier Assets:** These are valuable items used by the supplier to produce the product or service. They can be people, software, documents, finances, or hardware among others.

2. Proposal from the AEO perspective

3. Customer: is an individual, individuals, groups of individuals or organizations that consume the product or service made by the supplier.

4. Client Assets: they are valuable elements owned by the target.

2. Proposal from the AEO perspective

SUPPLY CHAIN ATTACK

For an attack to be classified as a supply chain attack, both the supplier and the customer must be targeted

Reason why these types of attacks are becoming more and more common

they provide adversaries with a significant reputational boost, as well as very likely large financial gains.

THE LIFE CYCLE OF AN ATTACK ON THE SUPPLY CHAIN

Two fundamental parts:

1. is the attack on the supplier: it focuses on compromising one or more suppliers.
2. is the client attack and focuses on the ultimate target of the attack.

2. Proposal from the AEO perspective

To work on risk management of AEO in their digital supply chains, it is necessary to characterize the attacks that have occurred

1. How the attack happened: techniques used against the supplier.
2. What was the target of the attack on the Supplier: asset(s) attacked that allowed more attacks to be carried out later.
3. How the attack happened: attack techniques used to compromise the customer through their supplier.
4. Primary and ultimate target of attackers, and often the rationale for a supply chain attack: targeted customer assets.

1. How the attack happened: Attack techniques used to compromise the supply chain:

Malware Infection, Social Engineering, Brute-Force Attack, Exploiting Software Vulnerability, Exploiting Configuration Vulnerability, Physical Attack or Modification, Open-Source Intelligence (OSINT) and Counterfeiting.

2. What was the objective of the attack on the supplier: asset(s) attacked that allowed further attacks to be carried out later:

Pre-existing Software, Software Libraries, Code, Configurations, Data, Processes, Hardware, People.

3. How the attack happened: attack techniques used to compromise the customer through their supplier:

Trusted Relationship, Drive-by Compromise, Phishing, Malware Infection, Physical Attack or Modification, Counterfeiting.

4. Attackers' primary and ultimate target, and often the rationale for a supply chain attack: targeted customer assets:

Data, Personal data, Software, software of the customer, Processes, Bandwidth, Financial, Intellectual property and People.

CONCLUSIONS

Supply chain attacks take advantage of the interconnectedness of global markets.

It is more, in terms of risk, when several AEO clients rely on the same AEO supplier; the consequences of a cyber-attack against this supplier are amplified, potentially resulting in a large-scale national or even cross-border impact.

Large-scale undermining both the strategic position of the AEOs directly involved in the attack, and the image of the entire AEO program.

CONCLUSIONS

The inherent global nature of digital supply chains geometrically increases the potential impact of attacks and broadens the attack window for malicious actors.

Additionally attacking the strategic position and the confidence generated from the AEO program.

RECOMMENDATIONS

To adequately manage the risks in the supply chain, AEO clients must advance and maximize the following practices:

- ✓ Identify and document the types of suppliers, preferring those AEOs for their business, defining risk criteria.
- ✓ Advance the evaluation of the risks of the supply chain in accordance with its own methodologies, obeying its AEO position.
- ✓ Define risk treatment measures based on good AEO practices.
- ✓ Define the security requirements for the products and/or services acquired, including all the obligations and requirements in the contracts; agree on rules for subcontracting and potential cascading requirements.
- ✓ Monitor service performance and conduct routine security audits to verify cyber security compliance; this includes handling incidents, vulnerabilities, patches, security, etc.

RECOMMENDATIONS

suppliers must:

- ✓ Ensure that the infrastructure used to design, develop, manufacture and deliver products, components and services follows cybersecurity practices, even surpassing AEO practices.
- ✓ Implement a product development, maintenance and support process that is consistent with AEO best practices.
- ✓ Conduct periodic audits to ensure compliance with the above measures.
- ✓ Monitor security vulnerabilities reported from internal and external sources.
- ✓ Analyze vulnerability risks by using a vulnerability rating system.
- ✓ Generate maintenance policies for the treatment of identified vulnerabilities based on risk.
- ✓ Implement processes to permanently inform customers.

THANKS !!

Sebastian Galindo Cantor
sgalindo@unal.edu.co

Gloria Rodríguez Lozano PhD., MSc.
girodriguezl@unal.edu.co