# 5.0 Supply Chains

A MNO's supply chain can be broken down into a number of components – from hardware to software - the parties involved in putting together products and services and the upkeep and maintenance of a network. Operational and support IT infrastructure networks are often composed of a variety of products and services from a wide range of suppliers.

Many jurisdictions classify mobile infrastructure as critical national infrastructure, and concerns about national security have increased the focus on the security posture of network equipment and the providers of it. National government responses vary from restricting certain vendors to implementing new defensive regulations / security requirements and attempts to broaden existing vendor arrangements via open networking and other non-proprietary technology initiatives.

Given the many opportunities and targets, supply chain attacks vary widely in nature. Some reported attacks include the following:

Attackers reportedly[29] used information obtained in a previous attack on password manager LastPass US to target a senior DevOps engineer with malware to "launch a coordinated second attack" that breached password vaults. This attack illustrates how reconnaissance and attack staging can be exploited at a later time.

A security breach was reported[30] at a third-party marketing partner of US operator AT&T that led to a compromise of customer proprietary network information, but no sensitive personal or financial information was accessed.

Lumen Technologies, which provides an enterprise technology platform that combines networking, cloud, security and collaboration services, has reportedly[31] fallen victim to attacks. A malicious intruder inserted criminal ransomware into some of the company's servers that support a segmented hosting service. A separate sophisticated intruder accessed some of the company's internal information technology systems, including conducting reconnaissance of these systems, installing malware and extracting a relatively limited amount of data.

## Analysis

In addition to the general pressure to diversify supply chains, restrictions (and in some cases bans) on using certain vendors is driving vendor swaps - so called rip and replace - in some markets. Whilst there may be advantages from a business reliance viewpoint, the origins and provenance of equipment and services are not a guarantee or substitute for good security. Furthermore, there is a need for balance to ensure any scale changes of vendor are achieved in a resilient, cost-effective manner and utilise robust alternative vendors.

[29] https://siliconangle.com/2023/02/28/lastpass-says-malware-used-hack-devops-engineer-2022-password-vault-breach/
[30] https://forums.att.com/conversations/att-mail-features/is-this-cpni-email-a-phishing-scam/64066deaac6ccc24bdf19e05
[31] https://d18rn0p25nwr6d.cloudfront.net/CIK-0000018926/32a7d44f-2b57-4acc-8307-665dedf21348.pdf

The selection and testing of new vendors/products is therefore a key activity. A common way of demonstrating product security is to build products that are independently assessed under globally recognised product security assurance schemes, such as the GSMA's Network Equipment Security Accreditation Scheme[32] (NESAS). These, in turn, can help avert fragmentation of regulatory security requirements by providing a globally-recognised robust security baseline that all stakeholders can adopt and adhere to.

Vendor selection is also important when considering managed service providers and providers of cloud services. It is crucial to understand the business reliance on these vendors, as they increasingly deliver parts of the security and operational models, introducing new threat vectors. The opportunity for indirect attacks through supplier or third-party tooling and services should not be underestimated and requires vigilance about which third-party tools to use, as well as awareness of the security posture of the third party. The potential force multiplier effect for an attacker across all the target's customers can make a vendor an attractive attack proposition.

The variety of significant supply chain incidents and supply chain threats[33] has prompted the publication of best practices that aim to mitigate supply chain risks. These are notably in the managed service provider area where there may have been implied customer/supplier and/or partner trust arrangements, rather than explicit and enforced security requirements. For example, ENISA has released[34] a supply chain cybersecurity good practices guide, and the UK's National Cyber Security Centre (NCSC) has also released a relevant guide[35]. The combination of government regulatory 'push' and the availability of increasingly valuable supply chain guidance ('pull') assist in the production and maintenance of meaningful and in-depth supply chain management plans. Software Bills of Materials[36] (SBOMs) and Hardware Bills of Materials[37] (HBOMs) can be used as a means to deliver, track and maintain clearer equipment and software supply chains, with additional benefits of tracking licensing and responding to any security vulnerabilities that emerge.

[32] GSMA | GSMA Network Equipment Security Assurance Scheme (NESAS) - Security
[33] For example, as reported in previous GSMA Mobile Telecommunications Security Landscape reports and examples earlier in this section
[34] Good Practices for Supply Chain Cybersecurity — ENISA (europa.eu)
[35] https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security
[36] https://media.defense.gov/2023/Nov/09/2003338086/-1/-1/0/SECURING%20THE%20SOFTWARE%20SUPPLY%20CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20SOFTWARE%20BILL%20OF%20MATERIALS%20CONSUMPTION.PDF
[37] https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management