CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
National Risk Management Center
December 2018

SUPPLY CHAIN RISKS for Information and Communication Technology

U.S. critical infrastructure relies on Information and Communications Technology (ICT)—defined by the National Institute of Standards and Technology as "the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information"—for daily operations and functionality. The Design, Development and Production, Distribution, Acquisition and Deployment, Maintenance, and Disposal phases of the ICT supply chain are susceptible to the malicious or inadvertent introduction of vulnerabilities such as malicious software and hardware; counterfeit components; and poor product designs, manufacturing processes, and maintenance procedures.

Exploitation of ICT supply chain vulnerabilities can lead to: system reliability issues, data theft and manipulation, malware dissemination, and persistent unauthorized access within networks. This infographic provides leaders at all levels of government and industry insight into how vulnerabilities can be introduced into the ICT supply chain, and the consequences of their exploitation.

1. DESIGN

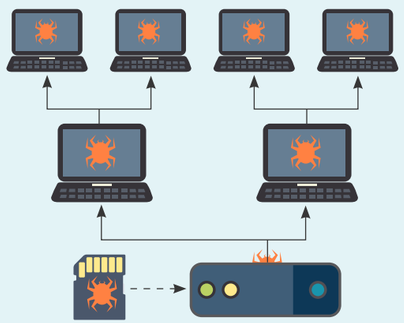
Vulnerabilities introduced during Design are often unintentional and can potentially affect all users of the components. Malicious actors could integrate vulnerabilities into components that may be installed in millions of pieces of equipment.

HIJACKED CELLULAR DEVICES

2016—A foreign company designed firmware used by a U.S. cell phone manufacturer. The phones made encrypted records of text and call histories, phone details, and contact information and transmitted that data to a foreign server every 72 hours.

2. DEVELOPMENT AND PRODUCTION

Vulnerabilities introduced during this phase are often inadvertent and can be costly to fix if not identified when testing initial prototypes. Well-designed products may still have malicious components introduced during manufacturing and assembly in a way that is potentially difficult to identify.



INFECTED SWITCH FLASH CARDS

2012—A third party factory that produced switches designed by a U.S. company installed infected compact flash cards during production. The U.S. company warned that using an infected component could compromise the system and potentially spread the malware within the network.

3. DISTRIBUTION

Components transported between production facilities and customers often do not fall under the purview of the personnel responsible for their design or production. Vulnerabilities introduced during Distribution are likely to be malicious and affect a limited number of components and customers compared to earlier phases.

END USER DEVICE MALWARE

2012—Researchers from a major U.S. software company investigating counterfeit software found malware pre-installed on 20% of devices they tested. The malware was installed in new desktops and laptop computers after they were shipped from a factory to a distributor, transporter, or reseller.

4. ACQUISITION AND DEPLOYMENT

Malicious insiders may insert vulnerabilities or replace equipment with vulnerable components during acquisition or installation. Vulnerabilities introduced during this phase likely affect only a limited number of customers.

COUNTERFEITS SOLD TO U.S. NAVY

2015—A U.S. citizen imported thousands of counterfeit integrated circuits from China and Hong Kong, and resold them to U.S. customers, including Defense contractors supplying them to the U.S. Navy for use in nuclear submarines.

5. MAINTENANCE

ICT components receiving Maintenance are susceptible to vulnerabilities introduced through physical or network access, and from exploitation of previously unknown or unpatched vulnerabilities. Vulnerabilities introduced during Maintenance might be targeted against specific entities, but can affect many customers in the case of software updates.

MALWARE EMBEDDED WITHIN SOFTWARE SECURITY TOOL

2017—Malicious actors attacked a security software company by infiltrating its network and inserting code into security software. Installs and updates to the application landed in millions of personal computers. The attack targeted predominant IT company networks.

6. DISPOSAL

ICT components that are improperly disposed of can contain sensitive company or customer data. Malicious actors can also attempt to refurbish components and try to resell them as new. Used parts may be less reliable and prone to failure, or have malware installed.

SENSITIVE FEDERAL DATA LOSS

2010—An internal audit discovered that a federal agency was selling computers containing proprietary information. Certain devices failed sanitation verification tests and resulted in the release of sensitive federal agency data.