Communications Security Establishment | Centre de la sécurité des télécommunications

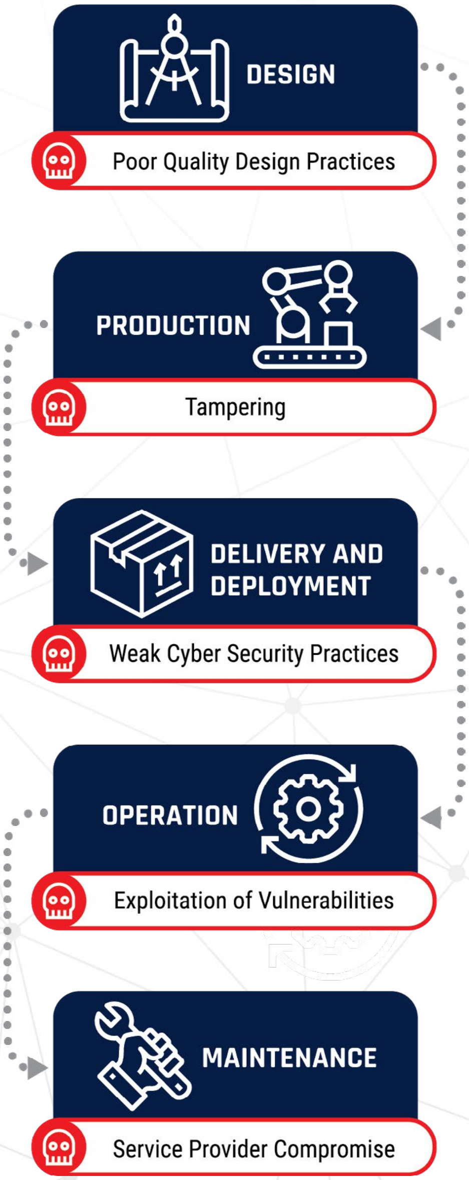
CANADIAN CENTRE FOR CYBER SECURITY | NATIONAL CYBER THREAT ASSESSMENT 2018

SUPPLY CHAIN THREATS AND COMMERCIAL ESPIONAGE

Supply chain refers to the processes required to design, manufacture and distribute equipment or other commodities, including information technology hardware and software. The stages of this complex process often involve different entities.

Supply chain security is only as strong as its weakest link. A security compromise anywhere in the supply chain could allow a cyber threat actor to exploit a device, or one of its components once it is connected to a company's secured network. Supply chains can be compromised before or after the delivery of a product or service, or during software updates or hardware upgrades.

Supply Chain Process


DESIGN
Poor Quality Design Practices
PRODUCTION
Tampering
DELIVERY AND DEPLOYMENT
Weak Cyber Security Practices
OPERATION
Exploitation of Vulnerabilities
MAINTENANCE
Service Provider Compromise

> ***"Every link in a global supply chain can pose a risk to cyber security "***

Threat actors may also exploit trusted relationships between businesses. For example, when multiple companies, contractors or business partners share access to critical data and networks an opportunity is created for cyber threat actors to access and exploit these shared networks and reach a desired target. Compromising many devices can help disguise a threat actor's motivation, identity and intended target.

State-sponsored cyber threat actors also advance their defence and technology sectors by conducting commercial cyber espionage around the world, including in Canada. This risk is even higher for Canadian companies that operate abroad.

WHAT IS THE GOVERNMENT OF CANADA DOING?

The Canadian Centre for Cyber Security works closely with stakeholders in critical sectors to provide advice and guidance to help mitigate supply chain risks in critical infrastructure that Canadians rely on every day.

For example, since 2013, the Communications Security Establishment's Security Review Program has helped mitigate supply chain threats to the telecommunications sector for 3G, 4G and LTE technology. To date, CSE and its government partners have worked with companies representing over 99% of the Canadian mobile market to help mitigate the risk of cyber espionage and network disruption. This program has helped mitigate risk by excluding designated equipment and services from sensitive areas of Canada's telecom networks.

TOP TIPS FOR BUSINESS OWNERS AND OPERATORS

- Ask partners, vendors, and other service providers questions about their security practices.
- Conduct vendor, partner, and other service provider risk assessments
- Protect information at the enterprise level. Security can be strengthened by establishing limited information or network access for relevant vendors
- Consolidate, monitor, and defend internet gateways
- Patch operating systems and applications
- Provide tailored awareness and training to employees
- For more go to cyber.gc.ca

Canada