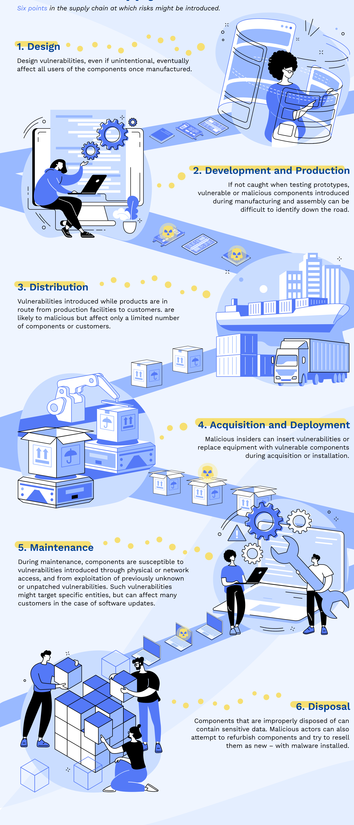
How to Close the Gaps in IT Supply Chain Security

The Department of Homeland Security has identified IT supply chain security as a national imperative. Given the extent to which agencies depend on commercial hardware and software, they cannot afford to ignore the risks posed by industry partners that do not protect against the injection of malicious code and components during the design, development and distribution of their products. GovLoop and HP created this infographic to look at the key vulnerabilities that agencies need to address.

End-to-End Supply Chain Risks

Six points in the supply chain at which risks might be introduced.



1. Design

Design vulnerabilities, even if unintentional, eventually affect all users of the components once manufactured.

2. Development and Production

If not caught when testing prototypes, vulnerable or malicious components introduced during manufacturing and assembly can be difficult to identify down the road.

3. Distribution

Vulnerabilities introduced while products are in route from production facilities to customers, are likely to malicious but affect only a limited number of components or customers.

4. Acquisition and Deployment

Malicious insiders can insert vulnerabilities or replace equipment with vulnerable components during acquisition or installation.

5. Maintenance

During maintenance, components are susceptible to vulnerabilities introduced through physical or network access, and from exploitation of previously unknown or unpatched vulnerabilities. Such vulnerabilities might target specific entities, but can affect many customers in the case of software updates.

6. Disposal

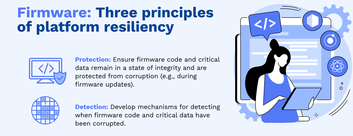
Components that are improperly disposed of can contain sensitive data. Malicious actors can also attempt to refurbish components and try to resell them as new – with malware installed.

Hardware: Mapping Out Supply Chain Risks

The Government Accountability Office highlighted the many potential sources of just five components that go into a standard laptop.

Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Firmware: Three principles of platform resiliency

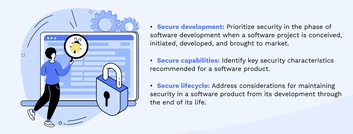


Protection: Ensure firmware code and critical data remain in a state of integrity and are protected from corruption (e.g., during firmware updates).

Detection: Develop mechanisms for detecting when firmware code and critical data have been corrupted.

Recovery: Develop mechanism for restoring firmware code and critical data to a state of integrity in the event of corruption.

Software Security: Three Points of Focus

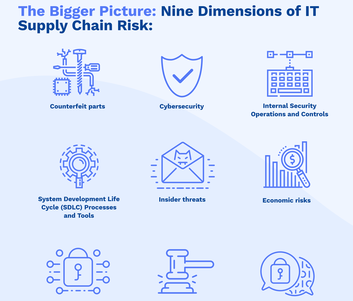


- **Secure development:** Prioritize security in the phase of software development when a software project is conceived, initiated, developed, and brought to market.
- **Secure capabilities:** Identify key security characteristics recommended for a software product.
- **Secure lifecycle:** Address considerations for maintaining security in a software product from its development through the end of its life.

Industry Partners: Four Questions About Supply Chain

- Is the vendor's software/hardware design process documented? Repeatable? Measurable?
- Is the mitigation of known vulnerabilities factored into product design (through product architecture, run-time protection techniques, code review)?
- How does the vendor stay current on emerging vulnerabilities? What are vendor capabilities to address new "zero day" vulnerabilities?
- What controls are in place to manage and monitor production processes?

The Bigger Picture: Nine Dimensions of IT Supply Chain Risk:



Counterfeit parts

Cybersecurity

Internal Security Operations and Controls

System Development Life Cycle (SDLC) Processes and Tools

Insider threats

Economic risks

Inherited Risk (Extended supplier chain)

Legal risks

External end-to-end supply chain risks (natural disasters, geo-political issues)

How HP Can Help

HP recently announced it is delivering the highest level of security for a growing number of U.S. federal and public sector customers that prefer U.S. sourced products with verifiable cyber assurance by expanding and further securing its supply chain. HP is the only major server manufacturer to produce made-in-USA industry-standard servers. The new servers include advanced security features that are built by vetted HP employees in highly secure U.S. facilities as part of the HP Trusted Supply Chain initiative launched today. Learn more here: www.hp.com