

# Software Supply Chain Security

Chris Fagan

Senior Director, Software Integrity Initiative

Microsoft Corporation

# Acquirer Perspective

## Acquirers Ask

- Where is code being developed?
- Is the software supply chain secure?

Acquirers are concerned about the safety and security of the software they rely on

# Supplier Perspective

## How do we define malicious code?

Malicious code is software inserted into an information system to cause harm to that system or other systems or to subvert them for use other than that intended by their owners

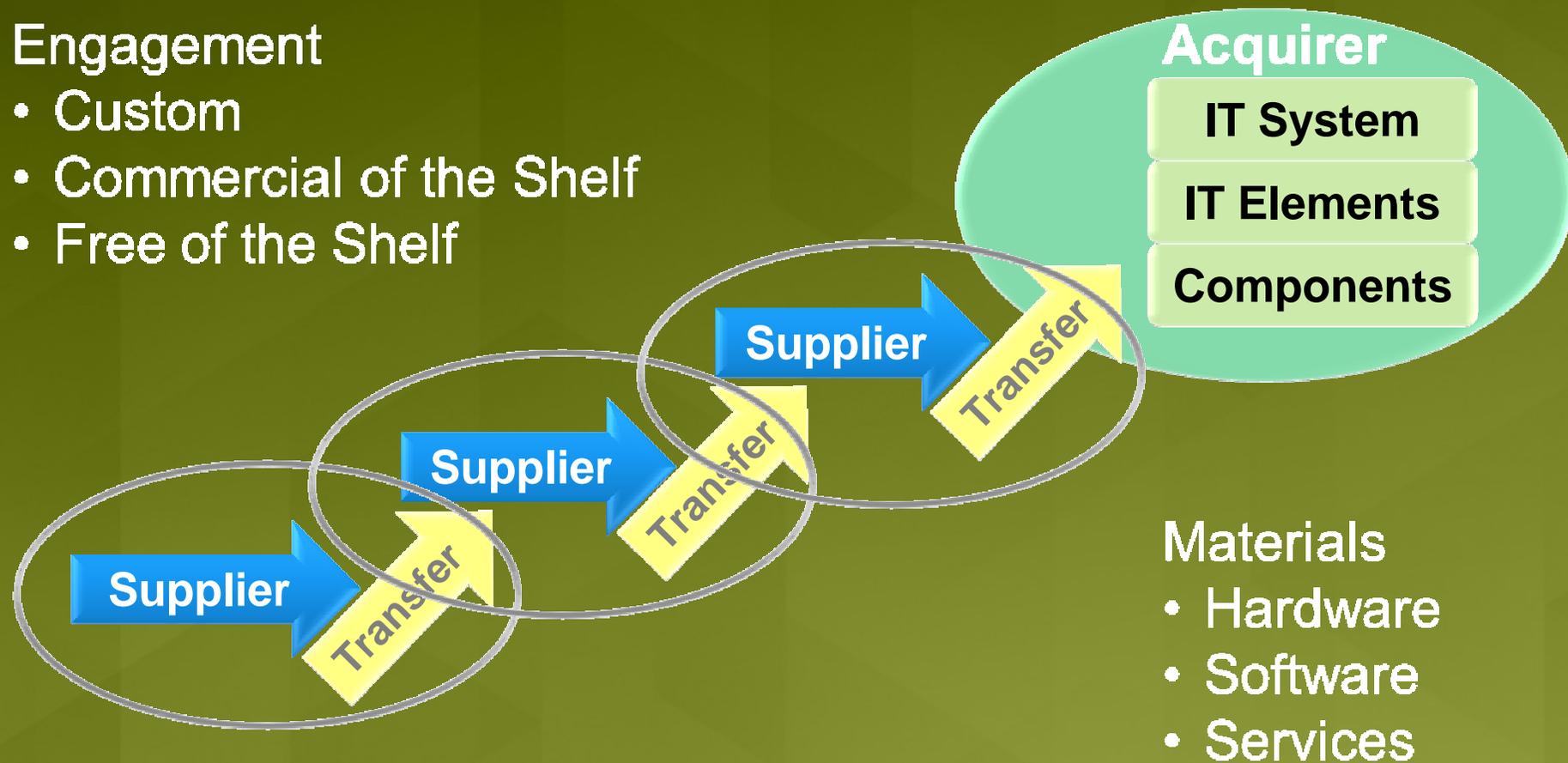
<http://www.oecd.org/dataoecd/53/34/40724457.pdf>

- **Malicious is not the same as:** software with a legitimate purpose that contains vulnerabilities
- **During development:** not at run time i.e. source or binary files, trap doors and Trojan horses

# IT Supply Chain

## Engagement

- Custom
- Commercial of the Shelf
- Free of the Shelf



# Software Supply Chain Attack

Bad Actor → Bad File

**Acquirers need assurances that software is:**

- **Sound:** i.e. the derivation of components is known and those with access are accountable
- **Secure:** i.e. security threats are anticipated by design, in development and deployment
- **Authentic :** i.e. not counterfeit, and that you can validate that you have the real deal