Microsoft | Trustworthy Computing

SECURE DEVELOPMENT IN THE SUPPLY CHAIN ERA

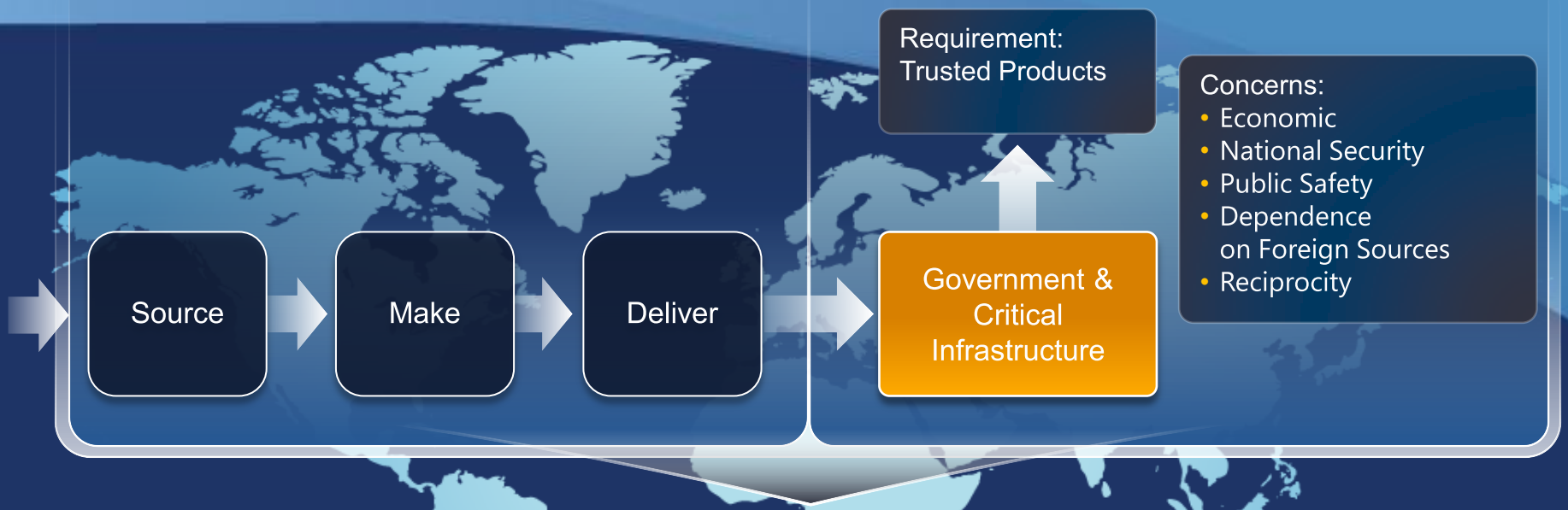
Ralph Hood
Group Program Manager, Security Engineering Strategy,
Trustworthy Computing
Microsoft Corporation

Cyber Threat Evolution

1986–1995	1995–2003	2004-2006	2006+
Characteristics			
• LANs • First PC virus	• Internet Era • "Big Worms"	• OS, DB attacks • Spyware, Spam	• Targeted attacks • Social engineering
Motivations			
Reputation, Damage…			
	Cybercrime		
		Economic/ Military Espionage	
			Cyber Warfare

Growing Government concern around supply chains delivering technology for national infrastructure

Supply Chain Complexity



Government Response

- United States → Defense Procurement Regulations; Draft Legislation
- Russia → Non-disclosed Functionality Policy; National Software Platform
- India → Indigenous Telecom Innovation Proposals
- China → 11th Five-Year Plan; Multi-level Protection Scheme (MLPS)

Industry Response

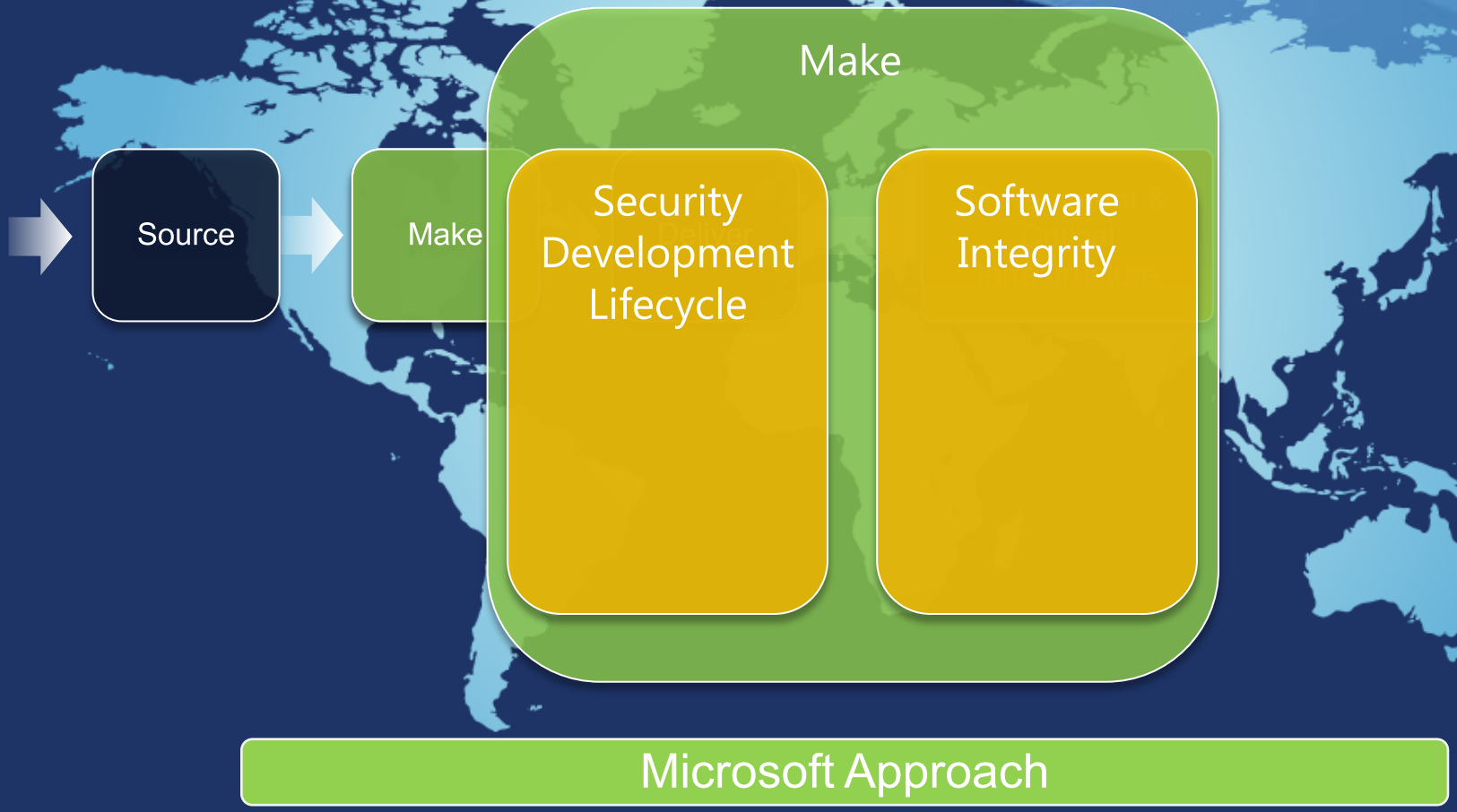
SAFECode — Software Assurance Forum for Excellence in Code — Driving Security and Integrity

THE Open GROUP — Making standards work®

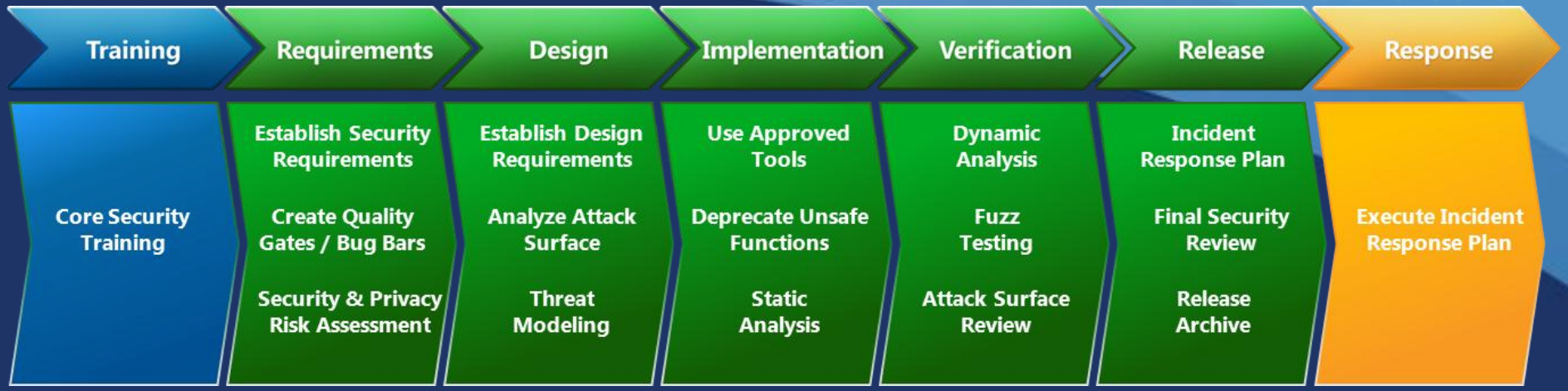
Open Group Trusted Technology Forum

TechAmerica — WHERE THE FUTURE BEGINS

Supply Chain Complexity

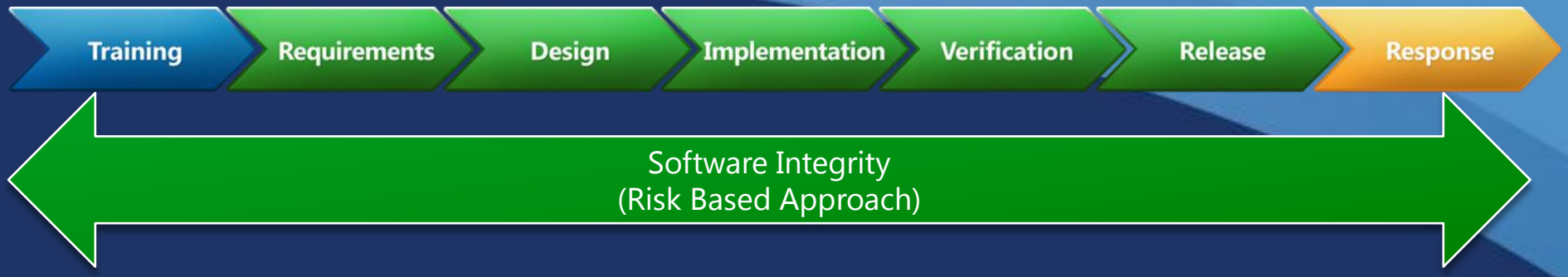


Security Development Lifecycle (SDL)



- Sixteen core processes from Training through Release
  - Integrates well with the existing Software Development Life Cycle (SDLC)
  - Strong reliance on automation
  - Includes activities for Architects, Program/Project Managers, Developers and QA/Testers
  - Note: Response not generally considered part of the SDL – but feeds into SDL
- Other non-development, post-release process requirements
  - Root cause analysis of found vulnerabilities; **failure of human, process, or automation**
  - Vulnerability analysis of similar applications
  - Penetration Testing as appropriate

Software Integrity



- We evaluate threats within software development model and focus on areas of significant risk (e.g., people, process, technology)
- Resulting Control Categories
  - Proof of Identity
  - Access Management
  - Development Process Controls
  - Build Process Controls
  - Malware Scanning
  - Code Signing

Guiding Principles

Establish multilateral models to address risks associated with unknown processes & safeguards

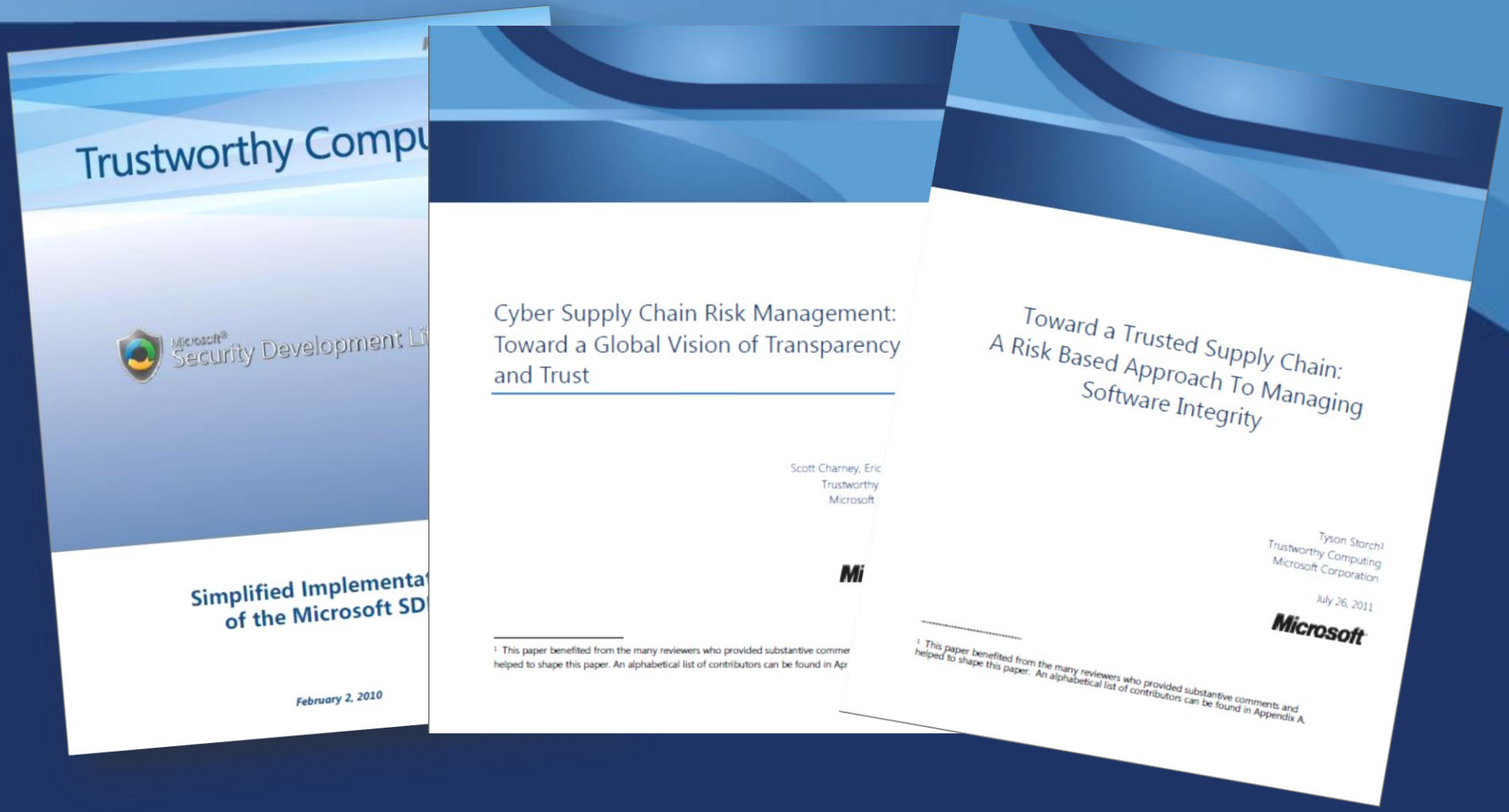
- Governments Develop a Risk Based Approach
- Private/Public Partnership Create Global Standards

Embrace Risk Based Approach

Ensure Transparency

Provide Flexibility

Recent Publications



More Information

- SDL Landing Page
  - http://www.microsoft.com/sdl
- SDL Simplified Whitepaper
  - http://www.microsoft.com/download/en/details.aspx?id=12379
- Supply Chain Whitepaper - Toward a Global Vision of Transparency and Trust
  - http://www.microsoft.com/download/en/details.aspx?id=26826
- Software Integrity Whitepaper - A Risk-Based Approach to Managing Software Integrity
  - http://www.microsoft.com/download/en/details.aspx?id=26828
- SAFECode
  - http://www.safecode.org/publications/SAFECode_Supply_Chain0709.pdf
- Open Group OTTF
  - http://www.opengroup.org/ottf

Microsoft®

Be what's next.™

© 2011 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.