Making the Invisible Visible

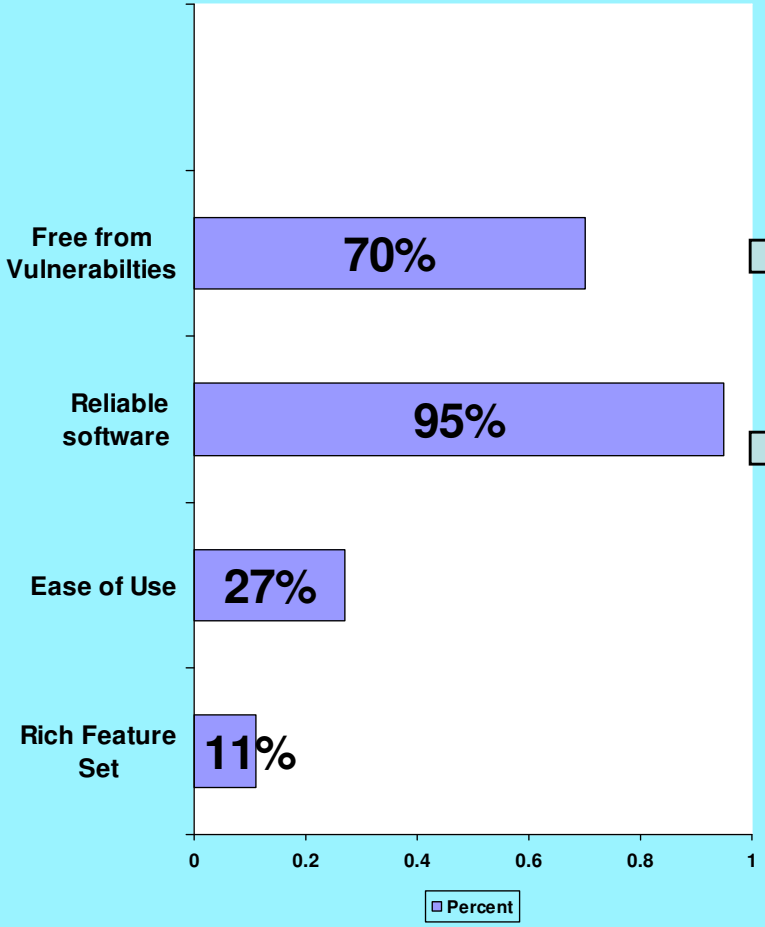
Gaining Visibility into Software to Achieve Assurance

"standards and metrics"

Daniel G. Wolf
Director
Software Assurance Consortium

SwAC
Software Assurance Consortium

CIO Executive Council 2006 Survey Software Consumer Priorities



Software Assurance (SwA)

Trustworthiness - No exploitable vulnerabilities exist, either maliciously or unintentionally inserted;

Predictable Execution - Justifiable confidence that software, when executed, functions as intended;

SwA
Software Assurance Consortium

So Why are We Here

- Private sector values assured software but makes purchasing decisions based on features and functionality

- Why:
  - Visible attributes, easy to understand and directly related to operation/mission
  - Software assurance is abstract, intangible and hard to understand
  - Software features are relatable to the software consumer

End Result: Quality of implementation does not drive purchasing decisions

SwAC
Software Assurance Consortium

What's Needed?
Standards & Metrics

- Standards provide a common lexicon to describing the invisible features of software assurance
- Metrics quantify the invisible attributes and makes them tangible

Enables informed purchasing decisions

SwAC
Software Assurance Consortium

Software Assurance Standards & Metrics Must be …

- Relatable to the software consumer
- Proactively guided by the consumer to ensure that they are practical and relevant to their operations

Otherwise

- Will not be broadly adopted
- May be misinterpreted
- May lead to faulty assumptions about operational risk
- May lead to false sense of assurance
- May result in rejection of standards and metrics as a viable business tool

SwAC
Software Assurance Consortium

Software Assurance Consortium

Bringing together Software Consumers, Industry, Academics, and Government to Transform the Security and Dependability of Software

Improve the overall software assurance:

- Provide a voice to articulate consumer needs
- Encourage adoption of standards, methods, metrics, tools, and other means for mitigating risks by software providers
- Identify successful practices, methodologies, and techniques
- Share experiences in choosing, developing, and implementing good code
- Encourage development, sharing and publicizing “best practices”
- Leverage other orgs to develop and deliver standards and metrics
- Define, prioritize and sponsor a SWA research agenda on the hard problems
- Apply standard measures of quality to address worldwide supply chain risk management

SwAC
Software Assurance Consortium

Why Software Assurance is Critical

- Software is the core constituent of modern products and services – it enables functionality and business operations
- Dramatic increase in mission risk due to increasing:
  - Software dependence and system interdependence (weakest link syndrome)
  - Software size & complexity (obscures intent and precludes exhaustive test)
  - Outsourcing and use of un-vetted software supply chain (COTS & custom)
  - Attack sophistication (easy exploitation)
  - Reuse (unintended consequences increases number of vulnerable targets)
  - Number of vulnerabilities & incidents with threats targeting software
  - Risk of asymmetric attack and threats
- Increasing awareness and concern

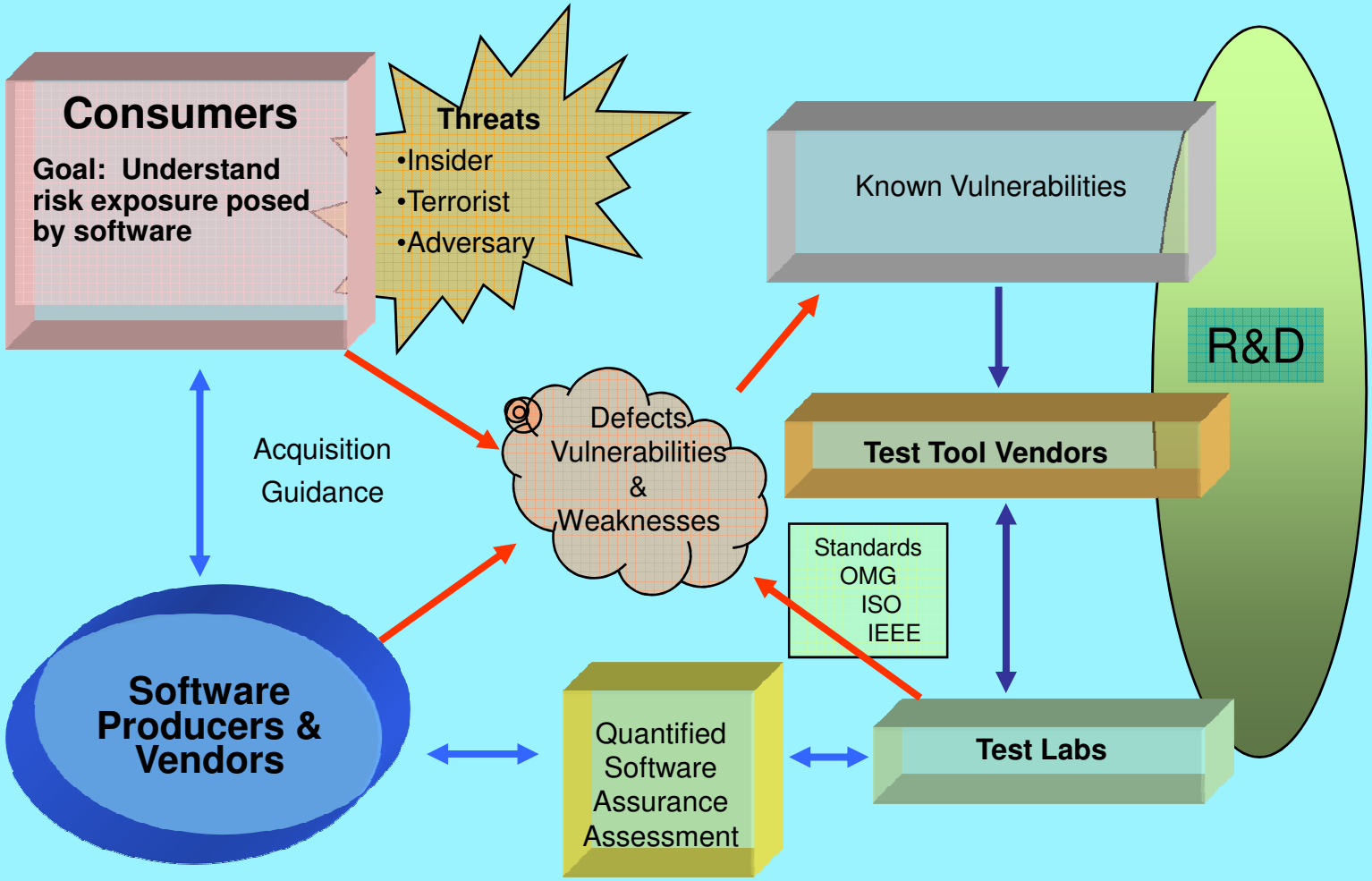
SwA
Software Assurance Consortium

SwAC Value for CIOs & Risk Managers:

- Be a voice for the consumer
- Strong voice to request special security features for small users
- Empower consumers to influence standards to improve SwA
- Provide a forum to share sensitive information
- Ability to report silently about what you don't want to say publicly
- Identify tools and testing labs: benchmark capabilities and features
- Provide special tools (propriety and sensitive) for the SwAC community
- Characterize the risk so you understand the potential impact
- Organizing formal and informal training for SwA
- Influence and improve SwA throughout the supply chain
- Satisfy Sarbanes Oxley for reasonable due diligence
- Develop a benchmark insurance, premium reduction considerations
- Software Facts Label (NIST)

SwAC
Software Assurance Consortium

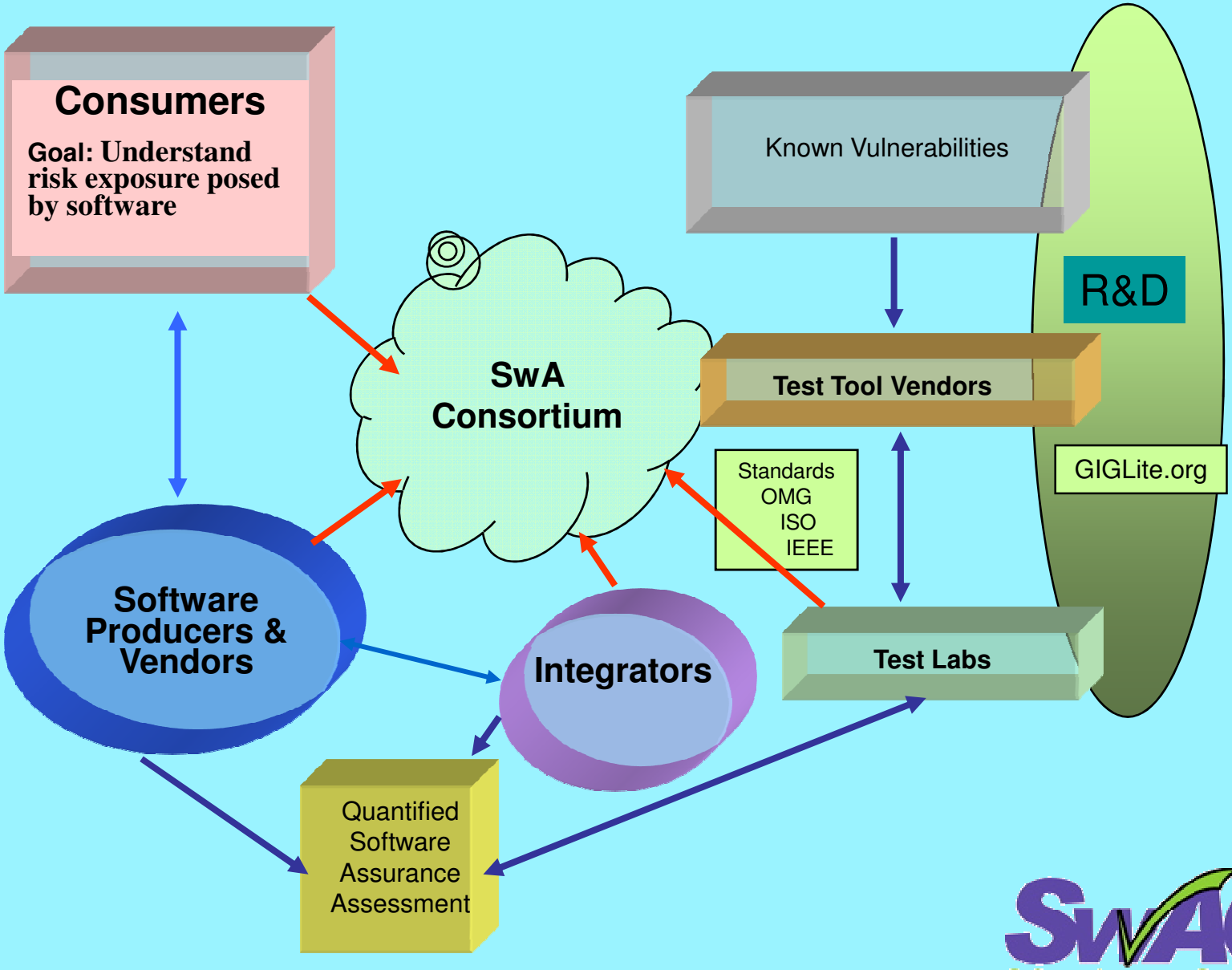
SwA Landscape



SwAC empowers software consumers to understand and reduce risk exposure attributable to software across the software supply chain.

SwAC
Software Assurance Consortium

Role of the SwA Consortium



SwAC
Software Assurance Consortium

Membership Categories

- Software end users
  - Commercial users
  - Integrators
  - Government users
  - Individuals
- Academic and research institutions
- Developers
- Liaison organizations
- Sponsors

SwAC
Software Assurance Consortium

Questions?

Membership Information:

Dan Wolf

Dwolf@CyberPackVentures.com

SwAC

Software Assurance Consortium