Agile and Cybersecurity – effective risk management is the key

Carol Woody, PhD

Will Hayes

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0441

Agenda

Cybersecurity for Software is Growing in Importance and Complexity

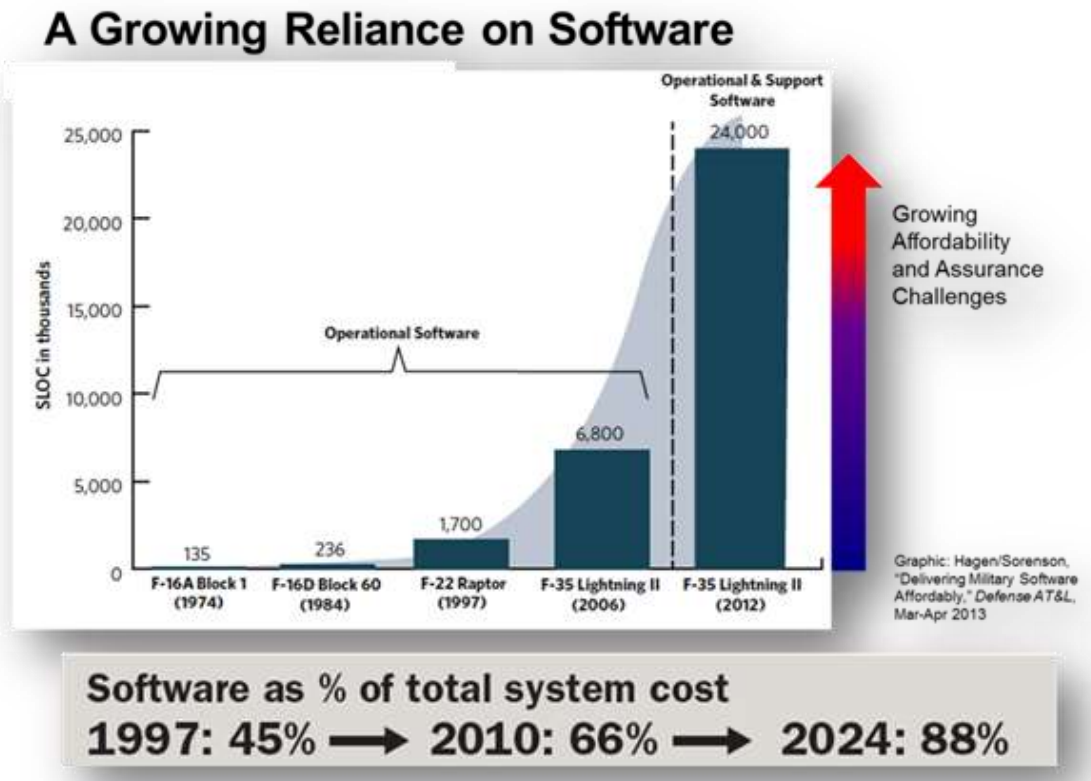
Agile at Scale with Quality

Addressing Cybersecurity Risk in Agile

Summary

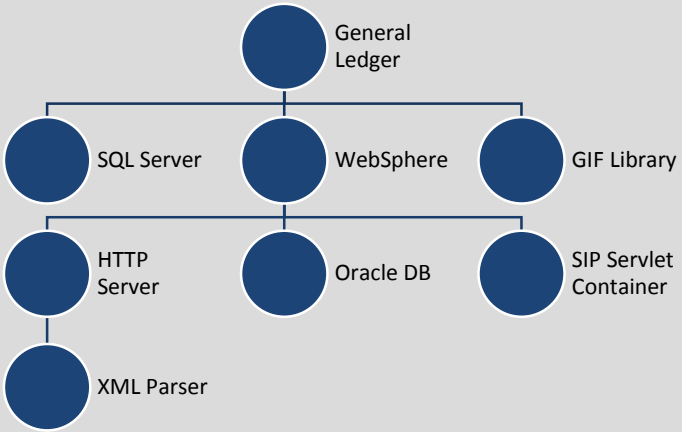
Cybersecurity for Software is Growing in Importance and Complexity

Software Investment and Reliance Is Rapidly Expanding



Source: U.S. Air Force Scientific Advisory Board. *Sustaining Air Force Aging Aircraft into the 21st Century* (SAB-TR-11-01). U.S. Air Force, 2011.

Software Development is Primarily Assembly



Note: hypothetical application composition

Process now involves assembly using collective development. Each product has

- too many components for a single organization to build all pieces
- too much specialization
- too little value in each individual component

Anyone Can Write Software

From 1997 to 2012, software industry production grew from $149 billion to $425 billion

From 1990 to 2012, business investments in software grew at more than twice the rate of all fixed business investments; from 2010 to 2012, software accounted for 12.2% of all fixed investment, compared to 3.5% for computers and peripherals

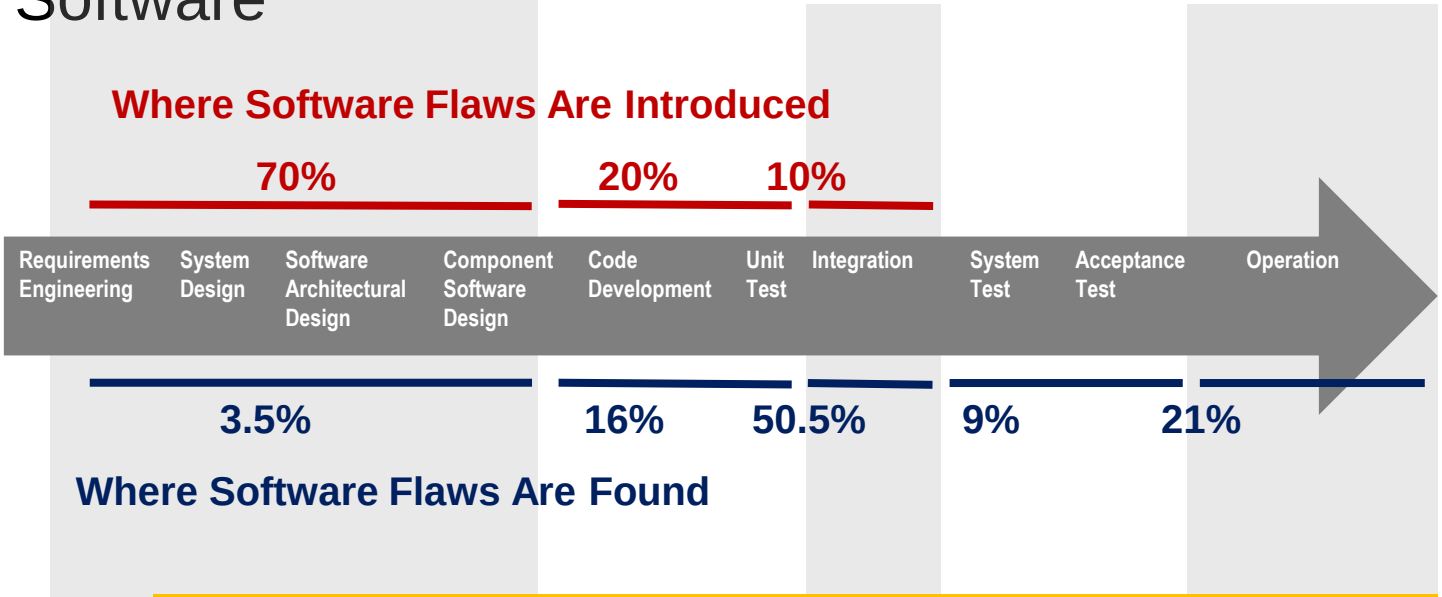
How to Raise the Next Zuckerberg: 6 Coding Apps for Kids
http://readwrite.com/2013/04/19/how-to-raise-the-next-zuck-6-coding-apps-for-kids/

TYNKER: We Empower KIDS to Become Makers
https://www.tynker.com/

How and Why to Teach Your Kids to Code
http://lifehacker.com/how-and-why-to-teach-your-kids-to-code-510588878

How do you make sure the code in your system is good?

Measure and Remove the Defects (and Vulnerabilities) in Software



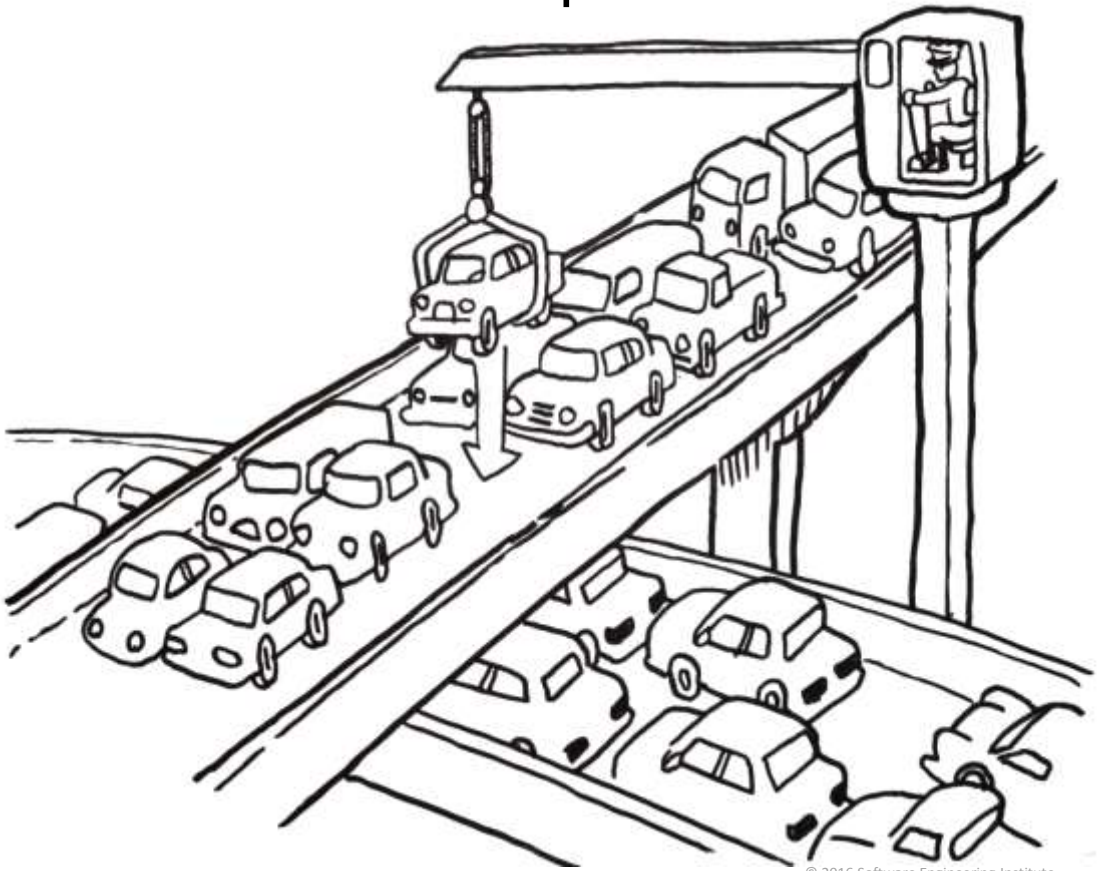
Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies

Best-in-class code: <600 defects per MLOC
Very good code: 600 to 1,000 defects per MLOC
Average quality code: 6,000 defects per MLOC

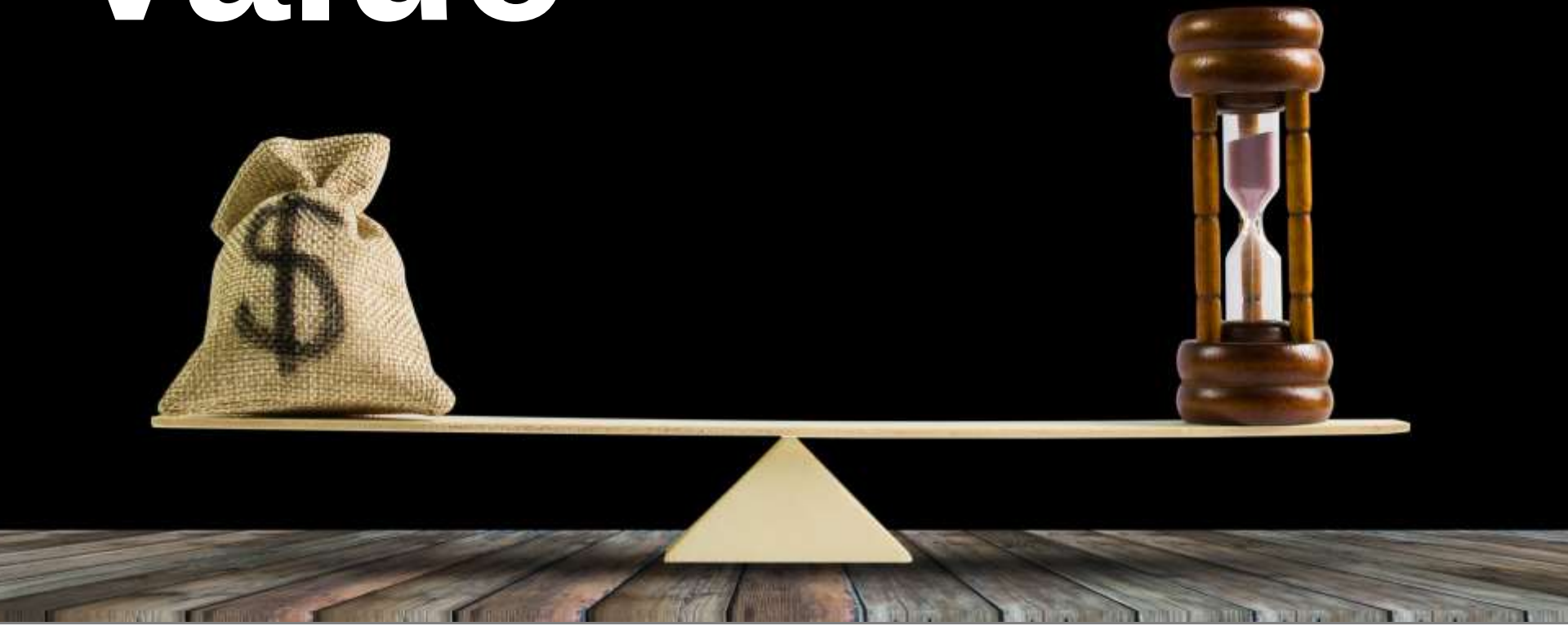
Up to 5% of defects are vulnerabilities

Agile at Scale with Quality

The Resource Utilization Trap



Value

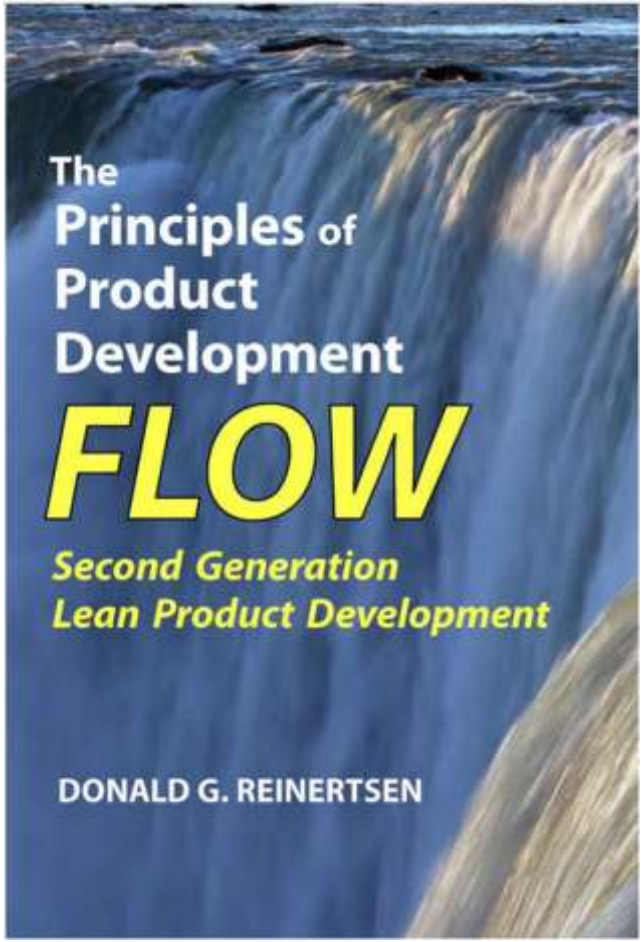


Cost of Delay

Reinertsen urges a focus on cost of delay, and proposed an approach to sequencing based on “Weighted Shortest Job First.”

Scaled Agile Framework (SAFe) elaborated the operational concepts shown below

$$\frac{\text{User-Business Value} + \text{Time Criticality} + \text{Risk Reduction and/or Opportunity Enablement}}{\text{Job Duration or Size}}$$



Defect Containment Modeling

		Detection Point									
		1	2	3	4	5	6	FQT	Injected in Sprint	Found Before FQT	Release Containment
Injection Point	1	35	13	8	5	3	1	1	66	65	98%
	2		35	9	7	5	3	3	62	59	95%
	3			35	12	8	2	5	62	57	92%
	4				35	18	4	8	65	57	88%
	5					35	5	12	52	40	77%
	6						1	5	6	1	17%
Found in Sprint		35	35	35	35	35	1	34	313	279	
Escaped Sprint		31	27	27	30	17	5				
Sprint Containment		53%	56%	56%	54%	67%	17%				

56%

Sprint Containment Effectiveness

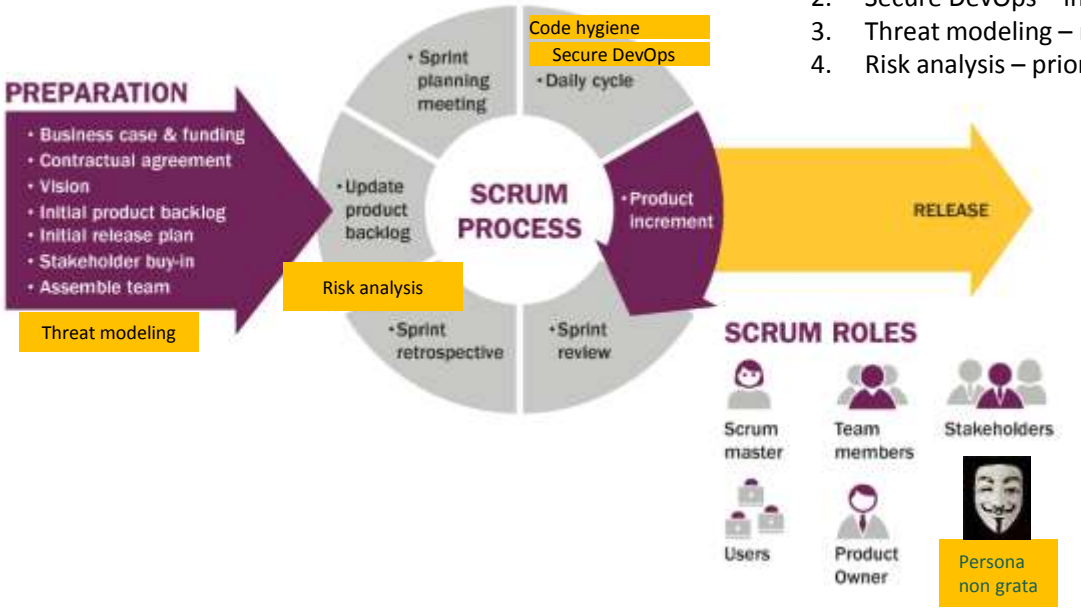
89%

Release Containment Effectiveness

Addressing Cybersecurity Risk in Agile

Integrating Cybersecurity into Agile (Scrum) Development

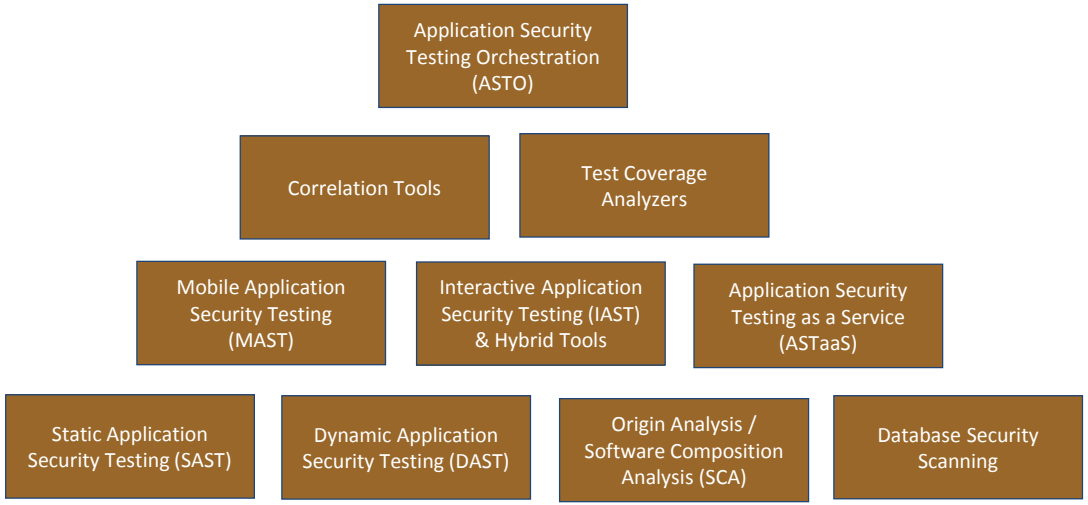
1. Code hygiene – introduce secure coding
2. Secure DevOps – include security tools
3. Threat modeling – represent a new role
4. Risk analysis – prioritize in backlog



(See also: Bellomo and Woody, DoD Information Assurance and Agile: Challenges and Recommendations Gathered Through Interviews with Agile Program Managers and DoD Accreditation Reviewers (http://repository.cmu.edu/cgi/viewcontent.cgi?article=1674&context=sei)

Improve defect containment for vulnerabilities

Classes of Automated Security Testing Tools for Code Hygiene and Secure DevOps



Reference: State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation (http://www.acq.osd.mil/se/docs/P-8005-SOAR-2016.pdf)

Threat Modeling and Risk Analysis

Threat Modeling: A Summary of Available Methods

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=524448

Example

The STRIDE approach to modeling threats was developed by researchers at Microsoft.

The name STRIDE is an acronym based on the initials of the threat categories: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.

An Approach for Integrating the Security Engineering Risk Analysis (SERA) Method with *Threat Modeling*

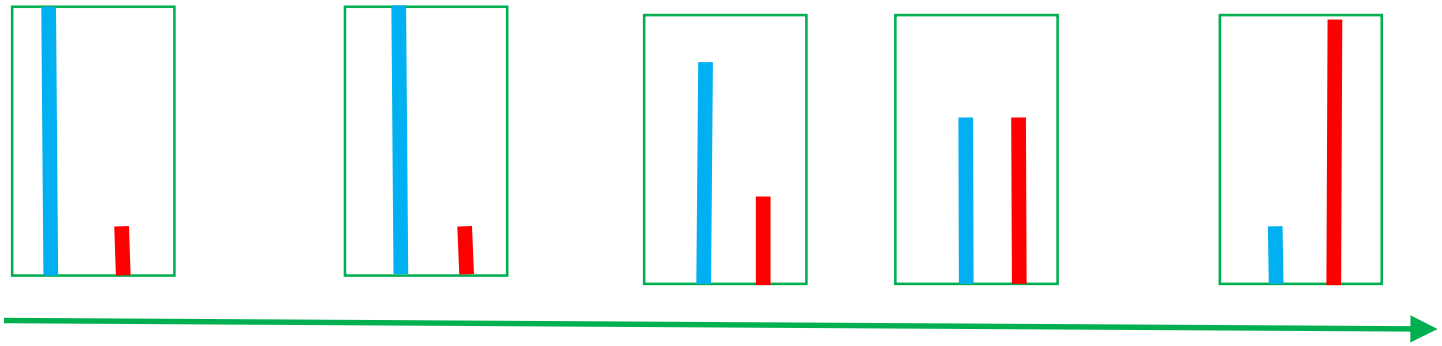
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=539808

Bring the Right Expertise at the Right Time

Resource levels for expertise vary across product releases as the product completeness grows

- Resources for cybersecurity (and safety)
- Resources for development

Traditionally cybersecurity expertise is not available until the product was finished. This does not provide sufficient expertise for integration of cybersecurity into Agile development



Summary

Cybersecurity Integration Requires a Shift in Emphasis

From primarily considering cost and schedule **to** an emphasis that values quality and security

From addressing security using compliance checklists for controls **to** effective and continuous identification and prioritization of cybersecurity risk based on the functionality delivered

From security testing when the product is done **to** continuous automated testing identifying and addressing cybersecurity weaknesses

From one-time consideration of security requirements **to** continuous and evolving consideration of cybersecurity risk as the product evolves

Resources

Carol Woody, PhD

cwoody@cert.org

Will Hayes

wh@sei.cmu.edu

Web Resources

www.sei.cmu.edu/go/cybersecurity-engineering

www.sei.cmu.edu/go/agile