Leveraging OWASP to Reduce Web App Data Breach Risk

PRESENTED BY
JOHN VERRY
PRINCIPAL SECURITY CONSULTANT
PIVOT POINT SECURITY

Specialists in Security Assessments, Penetration Testing,
ISO 27001 & Security Information Event Management

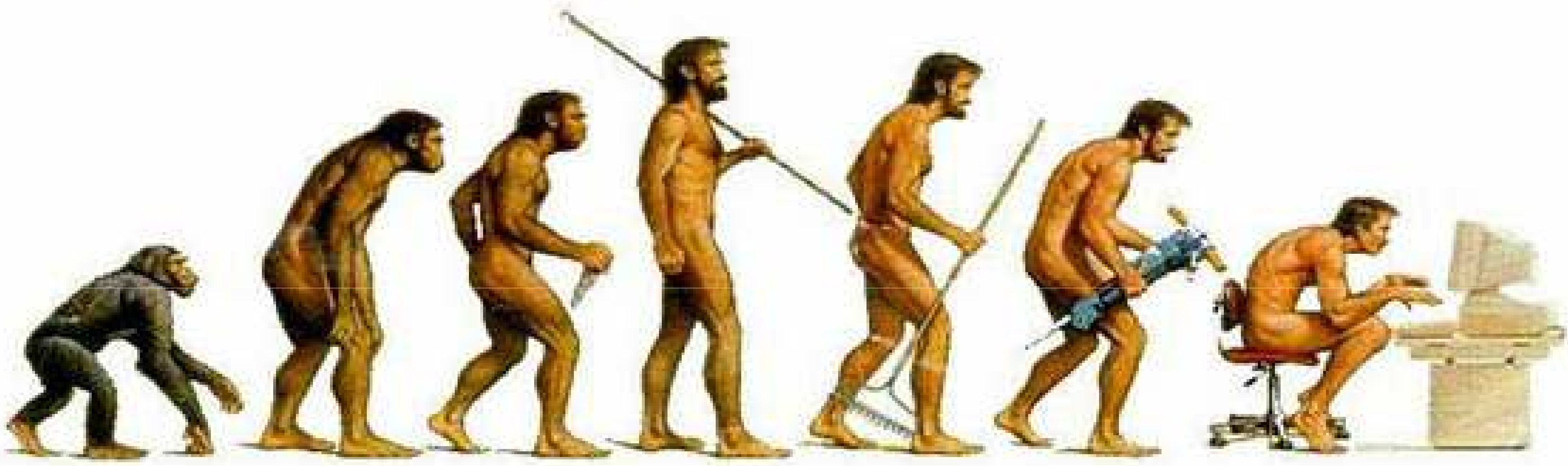
Webinar Value Proposition

Managing Risk in applications starts at the “top” and propagates throughout the organization

The quality and trustworthiness of available “good practice” has evolved significantly

- Leveraging these advances can provide significant advantages
- As you move forward ... you will view Pivot Point as a trustworthy entity

We need to Evolve …..



a process in which something passes by degrees to a different stage (especially a more advanced or mature stage)

… Change the Way We Respond to Threats

Tim Taddler, AP

Deploying more sophisticated technical controls ….

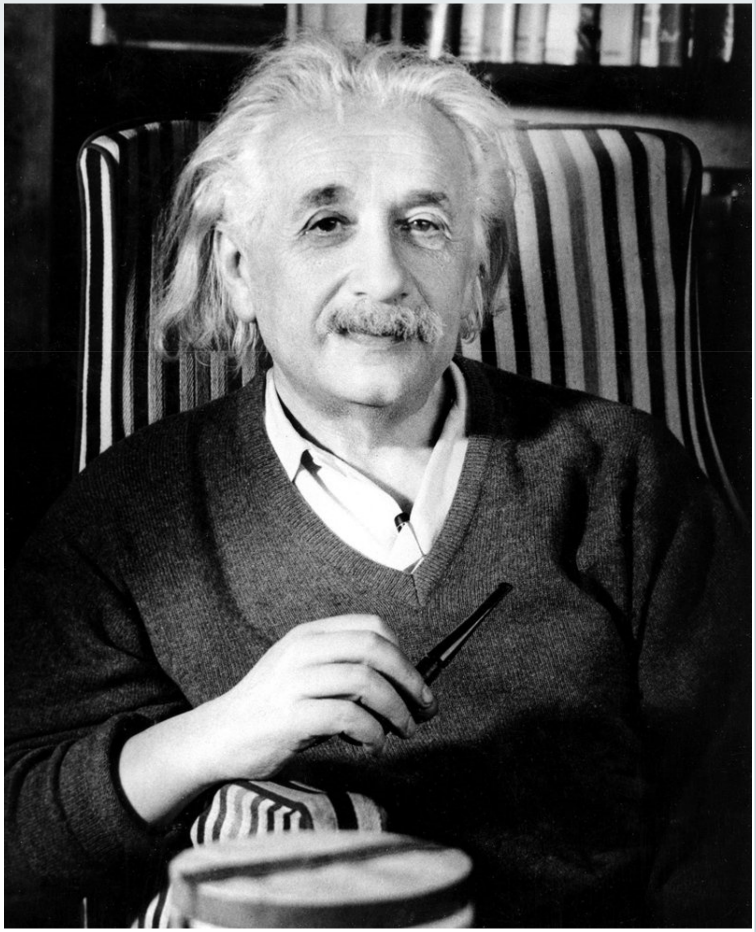
is not the answer

Occam’s Razor: Simplest is Best …

Occam's Razor: Simplest is Best …

"Simplicity is the ultimate sophistication."

"Make everything as simple as possible, but not simpler."



Common Sense – Address Root Cause

- ○ Insufficient education of key personnel
- ○ Understated understanding of risks
- ○ Poorly documented security requirements
- ○ Insufficient Certification/Accreditation Activities

Management’s failure to define (or enforce) a process (SDLC)

~~Root Cause “SQL Injection Attack~~”

Failure to Govern Creates a "Vacuum"

"Nature abhors a vacuum":

- Well intentioned people do well-intentioned things
  - But they often are not the "right" things
- Governance is ensuring that well-intentioned people *always* know the right thing to do

Establish AND Enforce a Process

Establish a **Security** Enhanced "Systems Development Lifecycle Methodology" (**S**SDLC)

Task an entity (e.g. Information Technology Steering Committee) with the responsibility to enforce it

Yea , Right ..
If It's So Simple Why Isn't Everyone Doing It?!?!

It is that "simple" ... but is is not Easy ... Why?

- Its not as much fun as implementing technical solutions

  What would you rather do - -spend a day piloting a new web application firewall or spending a day developing threat models

- "Rarely do we find men who willingly engage in hard, solid thinking. There is an almost universal quest for easy answers and half-baked solutions. **Nothing pains some people more than having to think."**
- We need to get "real work done" BAU and unrealistic deadlines prevent us from investing the effort
- Available Guidance has been very technical, fragmented and/or vendor/industry specific making it difficult to leverage

Fortunately – its getting easier!

OWASP Simplifies the Process

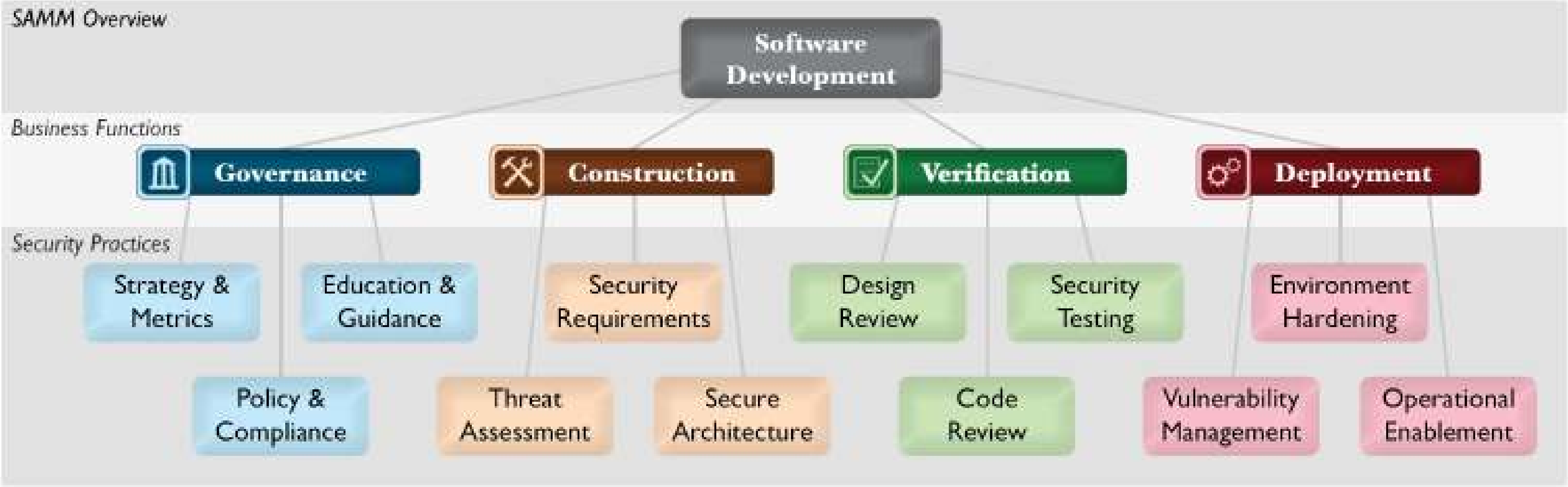
*Open Web Application Security Project – a n*ot-for-profit worldwide charitable organization focused on improving the security of application software

- *Have expanded from initial "Top 10 list" (2004) to the de-facto thought leader in Application Security*
  - *Publish "free & open" comprehensive guidance on the complete application lifecycle*

The Foundation: SAMM

Software Assurance Maturity Model – a framework to formulate/implement a strategy for software security tailored to your risk profile.

There are twelve core processes that must be addressed to a risk appropriate level



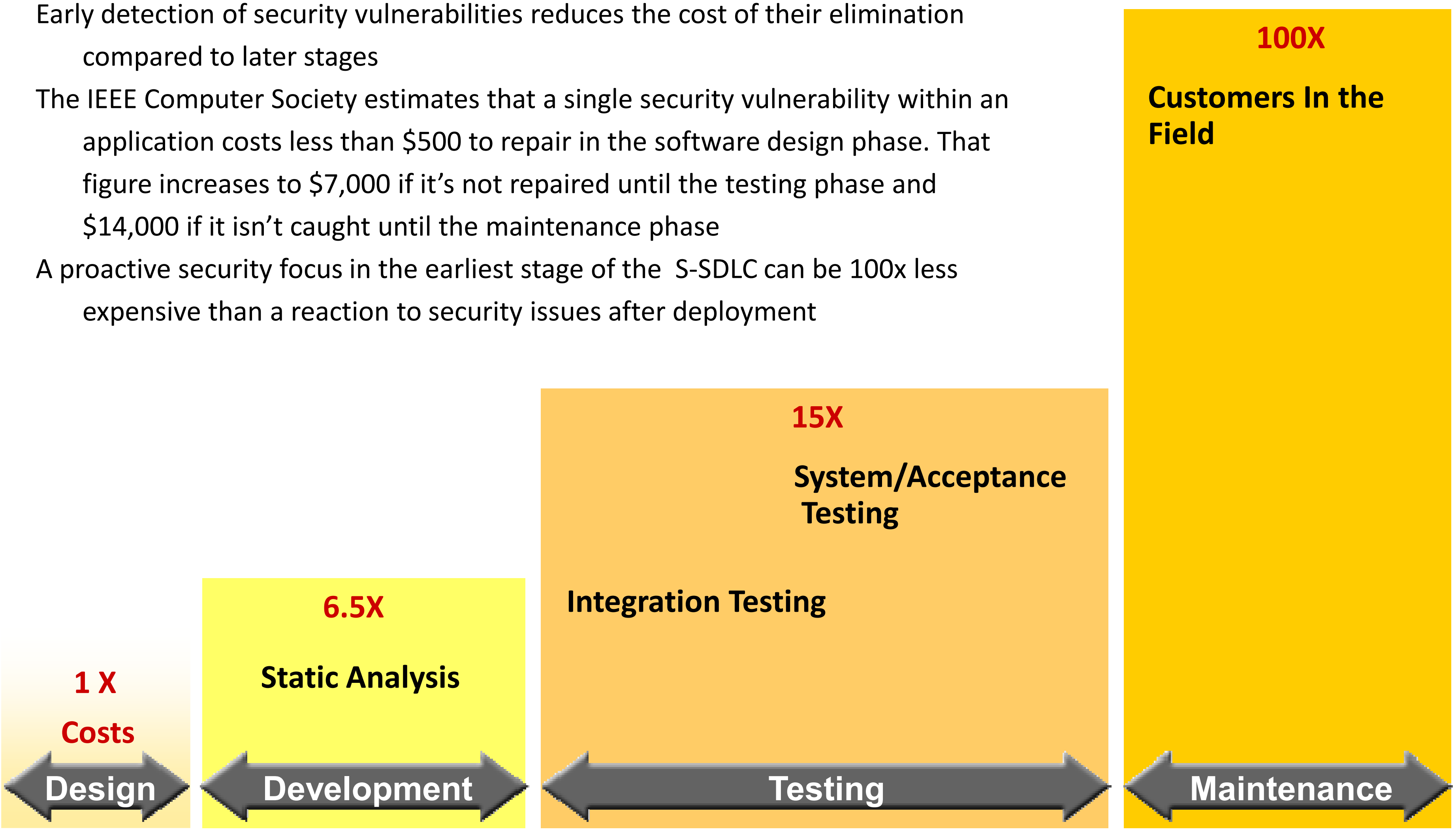
Approach to Security Cost Mitigation

There is value to addressing Security early in the Development lifecycle

Early detection of security vulnerabilities reduces the cost of their elimination compared to later stages

The IEEE Computer Society estimates that a single security vulnerability within an application costs less than $500 to repair in the software design phase. That figure increases to $7,000 if it's not repaired until the testing phase and $14,000 if it isn't caught until the maintenance phase

A proactive security focus in the earliest stage of the S-SDLC can be 100x less expensive than a reaction to security issues after deployment



1 X

Costs

Design

6.5X

Static Analysis

Development

15X

System/Acceptance Testing

Integration Testing

Testing

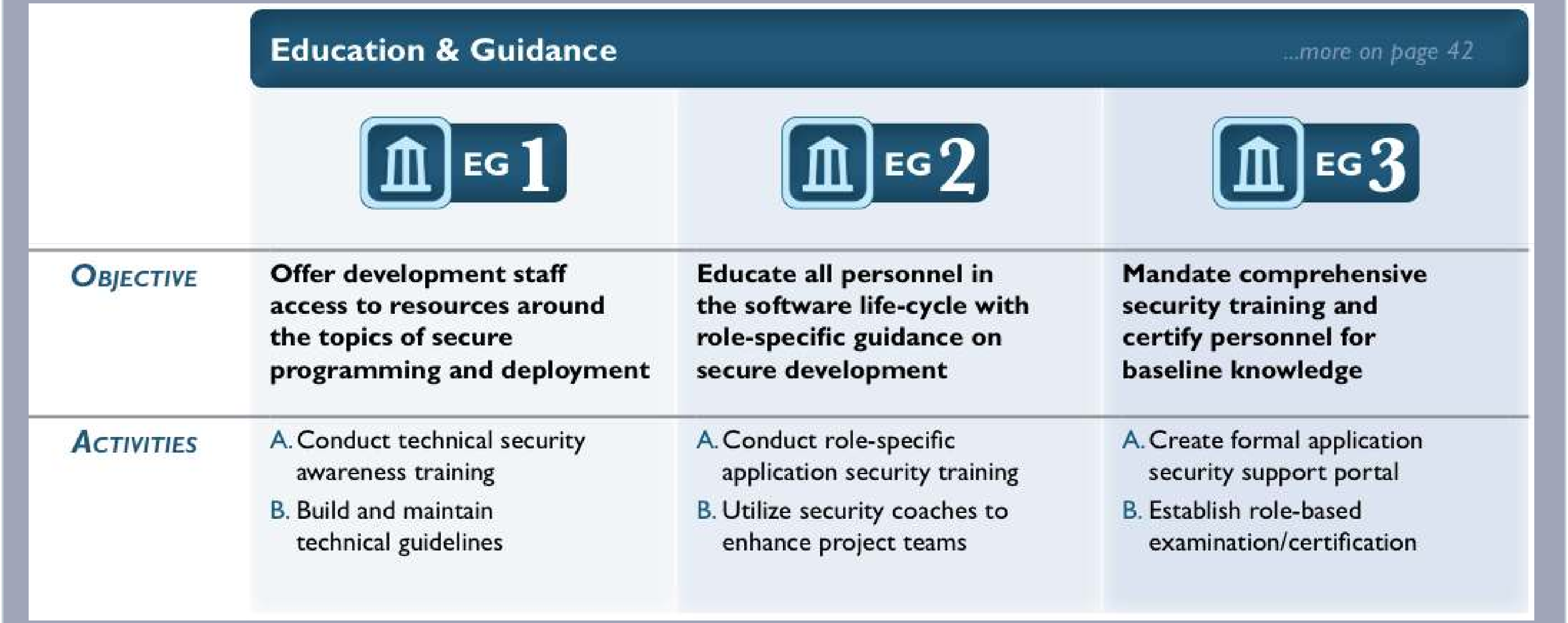
100X

Customers In the Field

Maintenance

Source IDC and IBM Systems Sciences Institute

An Example

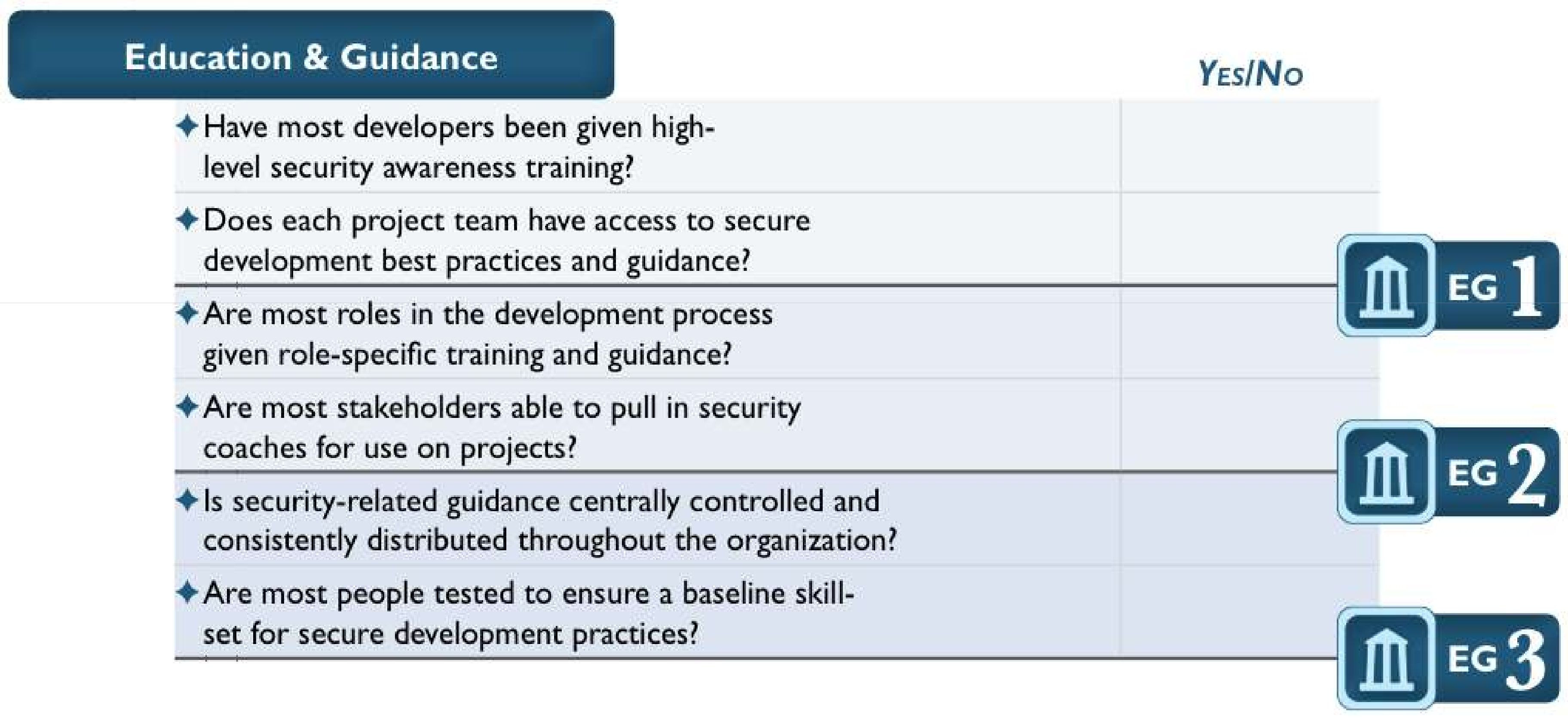


Education & Guidance

...more on page 42

	EG 1	EG 2	EG 3
OBJECTIVE	**Offer development staff access to resources around the topics of secure programming and deployment**	**Educate all personnel in the software life-cycle with role-specific guidance on secure development**	**Mandate comprehensive security training and certify personnel for baseline knowledge**
ACTIVITIES	A. Conduct technical security awareness training B. Build and maintain technical guidelines	A. Conduct role-specific application security training B. Utilize security coaches to enhance project teams	A. Create formal application security support portal B. Establish role-based examination/certification

SAMM: Implementation & Assessment Guidance



Education & Guidance	YES/NO	
✦Have most developers been given high-level security awareness training?		EG 1
✦Does each project team have access to secure development best practices and guidance?		
✦Are most roles in the development process given role-specific training and guidance?		EG 2
✦Are most stakeholders able to pull in security coaches for use on projects?		
✦Is security-related guidance centrally controlled and consistently distributed throughout the organization?		EG 3
✦Are most people tested to ensure a baseline skill-set for secure development practices?		

OWASP: Comprehensive Coverage

Governance

- **OWASP Top 10**
- OWASP Legal Project

Construction

- OWASP Top 10
- OWASP Developers Guide
- OWASP Aniti Samy
- OWASP ESAPI

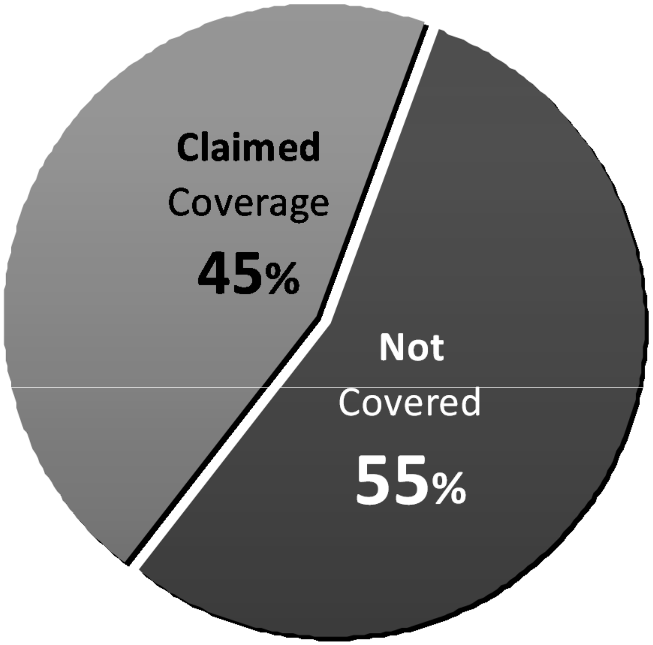
Verification

- OWASP Top 10
- **OWASP Application Security Verification Standard (ASVS)**
- OWASP Code Reviewers Guide
- OWASP Web Scarab
- OWASP Testing Guide

Deployment

- OWASP ESAPI
- OWASP WebGoat
- SAMM

Open Improves Trust



- MITRE found that all application security tool vendors' claims put together cover only 45% of the known vulnerability types (695)

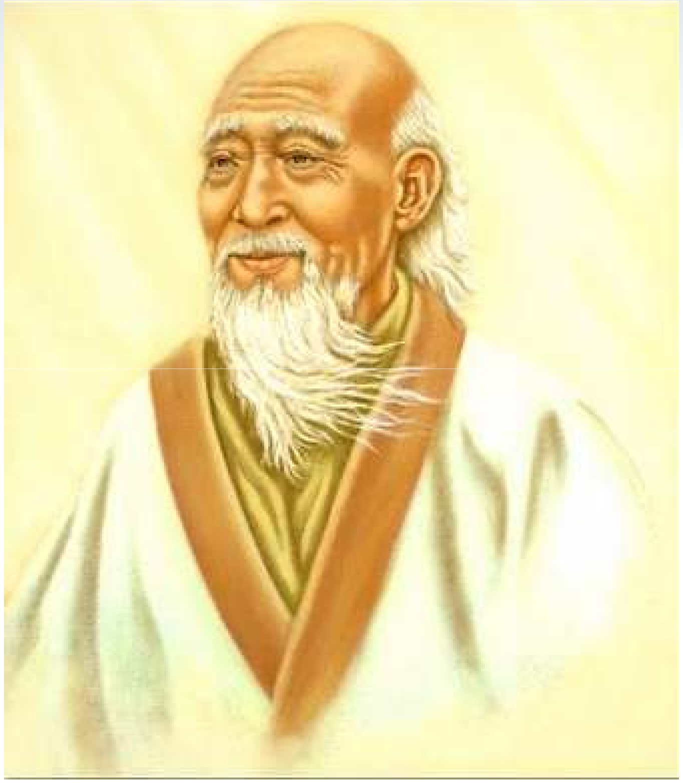
- They found very little overlap between tools, so to get 45% you need them all (assuming their claims are true)

SECURITYINNOVATION FORTIFY SOFTWARE PALAMIDA watchfire Klocwork Secure Software AppSIC CENZIC CORE SECURITY TECHNOLOGIES PARASOFT Coverity proServices SofCheck SPI DYNAMICS VERACODE OUNCE LABS

Slide Source : OWASP ASVS Presentation

Where Do We Go From Here?

"True wisdom seems foolish or childish." Lao-tzu



Where Do We Go From Here?

In a perfect world

- Evaluate your organization’s existing software security practices
- Build a balanced software security assurance program in well-defined iterations
- Demonstrate concrete improvements to a security assurance program
- Define and measure security-related activities throughout our organization

First Steps?

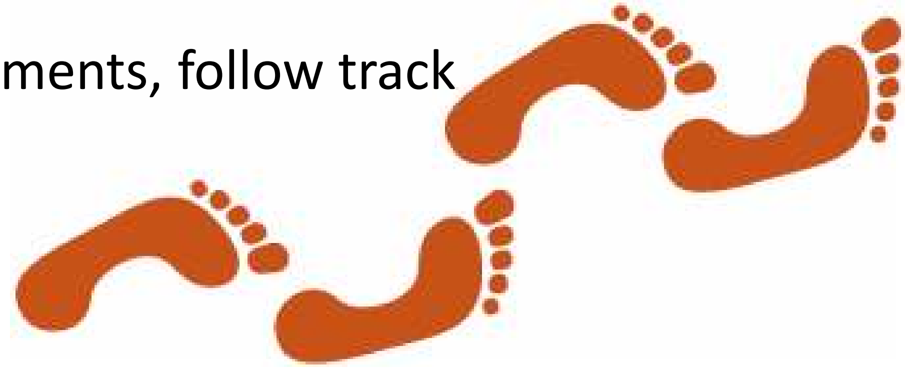
Reasonably Mature Software Development Practices in place and your existing high-risk apps have been subject to these practices

- Conduct a SAMM Gap Assessment and extend it to confirm SSDLC Governance
  - Leverage ASVS & Top 10 to maximum extent possible
- Close Notable Gaps
- Operate SSDLC with Continuous Improvement Principals

First Steps?

Immature Software Development Practices in place and your existing high-risk apps have been subject to these practices

- Conduct appropriate Verification Domain activities
  - Generally Vulnerability Assessment and Penetration Testing will be the most cost effective
- Remediate Deficiencies
- If deficiencies are significant, use findings to address upstream causes
- Post critical process improvements, follow track outlined in previous slide



A Couple of Considerations

OWASP is a great resource .. but …

- SAMM and ASVS are strong proponents of code scanning – which is fundamentally sound – but can be challenging
  - Code Scanners are often language specific
  - Code scanners can be expensive
  - Security Testing is often outsourced to a third party – which creates logistical challenges
- OWASP is very application centric
  - Still may need to leverage other security best practices to ensure total solution security

We are advocates of leveraging 27001 or derivatives of the same such as HITRUST and Shared Assessments

Did We Accomplish Our Agenda?

“Tone at the Top” is critical to managing risk

Leveraging good practices – especially OWASP -- can simplify the process and provide significant advantages

Should you look for external support – you will consider Pivot Point Security