Wild, Wild West

How to Corral All Your Developers into Creating Secure Code

Jonathan Beck
Static and Dynamic programs are great at finding vulnerabilities.

Penetration Test performed to deeply inspect applications.

Provided generic security requirements to all development efforts.

Correcting found issues was the responsibility of the development team.
Original State Issues

- Defects are discovered at the stage in the development lifecycle in which it costs the most to fix.
- The Developers are expected to halt their current development effort to address vulnerabilities.
- Developers are not given proper support to fix the issues quickly and competently.
Best practice sets you in the correct direction but it is not a map

- Develop Application Security Expertise
- Application Security Training and Awareness
- Risk Analysis
- Threat Modeling
- SDLC Integration
- Security Requirements
- Requirements Validation
Application Security Coaches
International Teams of Mystery

- Over 1,500 Developers
- Located in several countries
- Coding in Java, JavaScript, JSP, C, #, ++, PHP, COBOL, Perl, .net
- Using jQuery, Spring, Dojo, Struts
- Lifecyle HP ALM, M. Team Foundation, IBM Rational, Eclipse
International Teams of Mystery

- Supporting 7 major Lines of Business (LOBs)
- 1,000’s of applications
- 1,000’s of financial instruments
- Servicing millions of customers in 19 states
- Like piña coladas and getting caught in the rain
- Organized by LOBs, very little centralized representation
How we sometimes envision “Silos”
Darwin’s Developers
Application Security Coaches
Application Security Coaches

- Background in education
- Focus on building code, not tearing apart
- Working knowledge of all major languages
- Expertise in remediating security vulnerabilities
- There only job is to assist developers
Application Security Training and Awareness
App Security Training and Awareness

- **Audience**
  - Developers
  - Developing Tech Leads
  - Managers
  - Quality Assurance
  - Business System Analysts

- **Initial goal of 5 hours a year**

- **Training Effectiveness?**
  - Live instructor-led training
  - Virtual classroom with instructor
  - Self-paced computer based training (CBT)
  - Non-electronic courses
The New Normal

- People’s preference varied greatly
- Instructor led usually deemed the most effective
- Reoccurring theme was concern over not having enough time to complete training and being forced to take training in a format they do not like

I tried to be normal once.

Worst two minutes of my life.

- unknown
Taking a “Campaign” Approach

- Embracing the reality that one awareness solution is not going to get us to our desired state. Rather we need to create a tapestry of techniques, lining up the best qualities of each to meet the needs of all audiences.
- Nudging not nagging
- Example campaign elements
  - Community Portal
    - An interactive forum administered by Security Coaches to discuss new threats and vulnerabilities,
    - Awareness articles and security refreshers.
  - Communications celebrating team successes
Taking a “Campaign” Approach

- Presentations in senior management meetings
- Executive Support
- Training Program
  - Customized for each role
  - Combination of mandatory and optional
  - Combination of CBT and instructor
  - CBT
    » Navigation, Voice Acting, Presentation, Coverage, Technical, Interactive, Testing, Service
  - Instructor Led
    » Topics that have been identified as best delivered in-person to affect the greatest behavior-change in participants. This will be decided through patterns that appear across development teams, survey results, online feedback, test results, and gaps in CBT
Risk Analysis
Risky Business

- Drives the nature and strength of required security controls
- This is very personal to an organization
  - Risk definition needs to align with other cyber, audit, technology, and enterprise risk designations
- Risk frameworks that can assist
  - Octave Allegro
  - Factor Analysis of Information Risk (FAIR)
  - Dread
Threat Risk Modeling
Threat Risk Modeling

- Process using design documents and usage scenarios to drive analysis from an attacker’s perspective
- Goes way past code, past architecture, out to include operational and business practices.
- Identify Trust Boundaries and assess their ability to withstand attack
- Can be very challenging for complex systems
- Requires expertise to facilitate the discussion
- Only perform on systems with high potential impact
SDLC Integration
SDLC Integration

- Create Security Requirements
- Requirements are integrated into design
- Testing is completed on Security Requirements
- Quality Gates in place to ensure completion
- SDLC adherence can range greatly between teams
Security Application Requirements and Validation
Secure Application Requirements

- OWASP Top 10 is great, but…
  - Not cover custom or architectural control

- Move to language and functionality driven requirements
  - Means will need to understand the application a bit more than before

- Requirements need to be maintained as threat environment changes

- Vulnerability scan results need to be folded back into our requirements
Control Validation

- Each security requirement needs to be tested just the same as business requirements
- Failures need appropriate risk signoff
In Conclusion

- Best practice is the start of your journey not the end.
- Go in with eyes open, studying and understanding evolutionary differences. Steamrolling over them trying to get to process nirvana will likely end in ruin.
- The engagement of all the roles we discussed is critical to our continuing battle for the delivery high quality and secure applications.
Thank You

Jonathan Beck
jonathan.beck@pnc.com