



March 7, 2011

How Do You Achieve Developer Buy-In for Your Software Security Initiative?

SANS AppSec Summit 2011, San Francisco, CA



Introductions

- Who Am I?
 - Mike Hryekewicz, Software Engineer, QA Department
- Standard Insurance Company
 - Headquartered in Portland, Oregon
 - Primary products:
 - Group disability insurance
 - Individual disability insurance
 - Group life insurance
 - Group dental insurance
 - Group accidental death and dismemberment insurance
 - Retirement plans
 - Annuities

Bridging the Culture Gap



How most security initiatives are implemented:

InfoSec: *“You don’t understand security!”*

Developer: *“And you don’t understand development!”*



Enlist QA as the intermediary:

QA: *“I understand requirements and testing to those requirements!”*

To keep your game running smoothly!



Establish Your Security Requirements

- What are the developers expected to defend against?
- What is QA assessing and testing against?
- OWASP Application Security Verification Standard (ASVS)



Properly Document Security Findings

- They're not vulnerabilities...
...they're defects!



- Program X failed to meet documented security requirement A.
- Log it in your defect management system and track it!

Engage the Developers in Threat Modeling

- They're less defensive about handling identified security issues when the code hasn't been written yet.
- Encourage group participation in the threat identification process.
- Developers are often more enthusiastic about remediating issues when they're identifying them.
- You're training the trainers.



Continuous Software Security Education

- A one-time security training course is soon outdated and soon forgotten.
- Developers incorporate new frameworks, architectures, and libraries into their solutions each year, which each bring along their associated vulnerabilities.
- Keep your defensive best practices current and train on them accordingly.
- New security training often reinforces their prior training (e.g. validate, validate, validate!).



Tools are Cool!

- Good developers will readily adopt security tools into their daily routines that increase the quality of their code and don't waste their time.
- Even more so if these tools identify performance or stability concerns within their applications.
- It strengthens the link between their security training and their development activities.



Don't Force Standards on Developers

- Information Security often sets the software security requirements...

...but developers need to be engaged in specifying the associated development standards for meeting those requirements in their specific environment.



- OWASP ESAPI (Enterprise Security API) is a great start, but requires thoughtful integration into your frameworks.
- Developers are more likely to comply with standards that they own and contribute to.

Questions?

TheStandard[®]

Mike Hryekewicz
mhryekew@standard.com

The Standard is the marketing name for StanCorp Financial Group, Inc. and its subsidiaries. Insurance products are offered by Standard Insurance Company of Portland, Ore. in all states except New York, where insurance products are offered by The Standard Life Insurance Company of New York of White Plains, N.Y. StanCorp Equities, Inc., member FINRA, distributes group annuity contracts issued by Standard Insurance Company and may provide other brokerage services. Third-party administrative services are provided by Standard Retirement Services, Inc. Investment advisory services are provided by StanCorp Investment Advisers, Inc., a registered investment advisor. Commercial real estate loans are originated, underwritten and serviced by StanCorp Mortgage Investors, LLC, and a network of commercial mortgage banking correspondents. Product features and availability vary by state and company, and are solely the responsibility of each subsidiary.