Compliance, Security, & Innovation: Can They Co-Exist?

SANS AppSec 2013
Agenda

• My perspective
• What is Compliance
• Security and Innovation Issues
• Strategies to address Issues
• Questions?

Josh Brown-White
http://www.AnalyticalEngine.net
Always take anything a speaker says with a grain of salt, regardless of their experience, but...

• Sr. Application Security Architect, ~10 years of product security experience

• Currently Employed by ADP – world’s largest provider of Payroll and HR services, Vehicle dealership and automotive software. Also, dipping toes in medical provider software

• ADP has gobs of sensitive personal info, financial information, money movement info, etc.

• ADP does business in ~ 104 countries, physical presence in ~65 countries

• So compliance concerns tend to crop up fairly frequently for me

Josh Brown-White
http://www.AnalyticalEngine.net
Conforming to a specification, law, standard, or policy

- Government mandated law or requirement (SOX, HIPAA)
- Industry imposed regulation (PCI)
- Client/Partner contractual obligations
- Court ordered requirements (EU vs. Microsoft)
- Standards Interoperability (ISO, NIST, IEEE)
Security and Innovation Issues

• Requirement is specifically counter-security
• Requirement lead to weaker controls
• Requirement dictates specific implementation/technology
• Efforts to be compliant impact other work
• Compliance gets equated with security
• Compliance directs everyone to think a certain way
Strategies to Address Issues

• Get the right people
• Understand Intent
• Make compliance someone else’s problem
• Stack Controls
• Limit scope as much as possible
• Look for loopholes
• Get exceptions
• Lobby for change (figuratively and literally)
Contact Info

Twitter: @JBW_1

Email: joshbw@analyticalengine.net