RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: GRC-W10

Getting Off the Hamster Wheel of Testing

MODERATOR: **Wendy Frank, Principal Cybersecurity, Privacy & Risk, PwC**

PANELISTS:

Diana Kelley
Global Executive Security Advisor
IBM Corporation

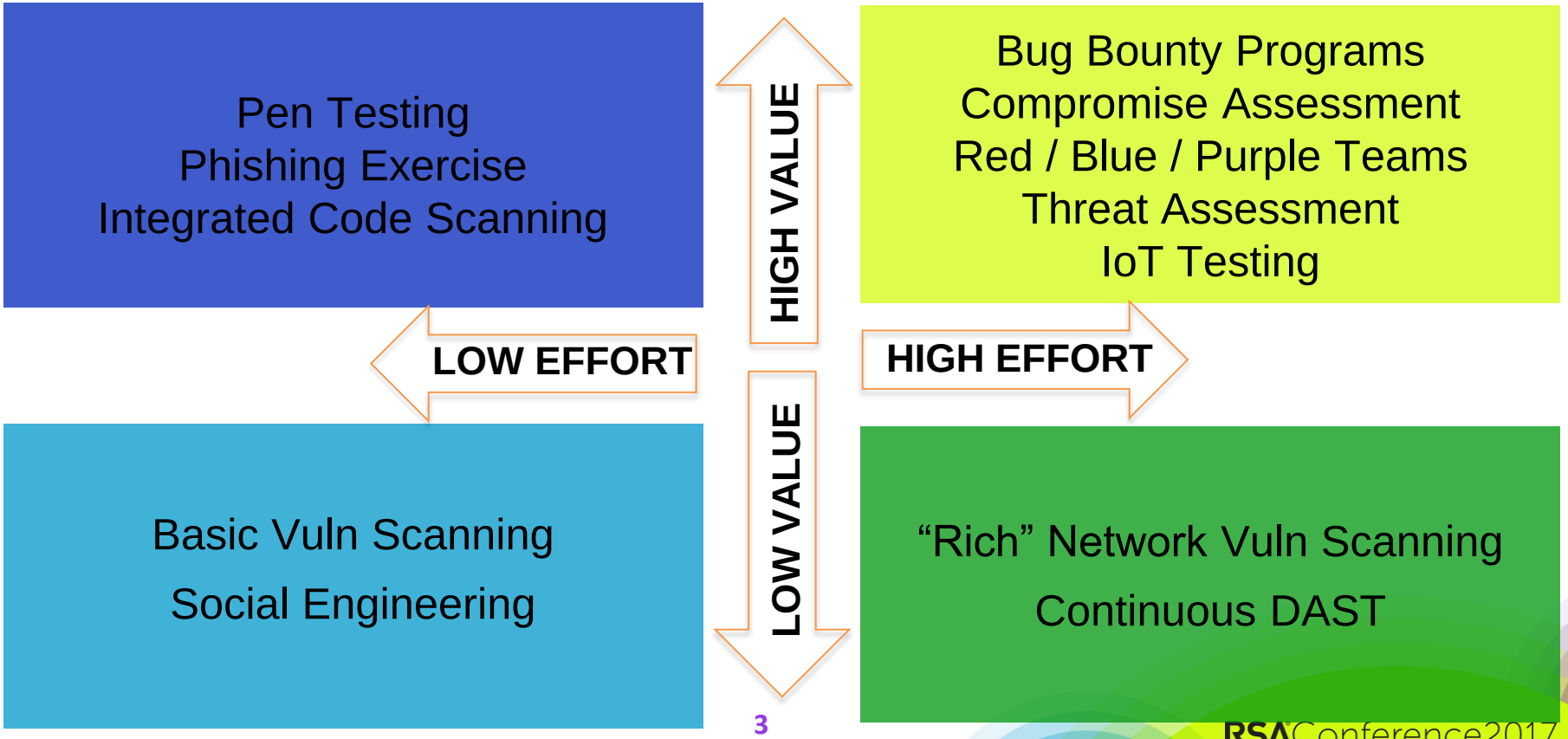
Lisa Lee
IT Examiner
Office of the Comptroller of the Currency

Latha Maripuri
SVP and Global CISO
News Corp

Agenda

- The Good, The Bad, and The Ugly
- Impact vs Effort
- Maturity Model of Testing
- Off the Wheel… Next Steps

Impact vs. Effort



Maturity Model of Testing

	Blissful Ignorance		Early Maturity		Threat & Risk Testing	
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Asset Inventory	None	Basic	More complete	Complete on prem	Robust - on prem/cloud	Robust - on prem/cloud
Vulnerability Scanning	None	Infrequent/via 3rd party	Regular but not often	Self-scan; often	Self-scan; frequent	Frequent
Social Engineering	None	None	Basic	Digital & Physical	Advanced Digital & Physical	Advanced Digital & Physical
Phishing	None	Basic	Scenario testing	Multiple scenarios	Multiple scenarios	Multiple scenarios & social technologies (FB, Twitter…)
Physical	None	None	Entry point testing	Entry point & interior	Entry point, interior, & eavesdropping scanning	Entry point, interior, eavesdropping, senior exec threat assessment
Ethical Hacking (Pen Tests)	None	Via 3rd party; infrequent	External & internal via 3rd party	Self & 3rd party; test at launch/change	Robust & frequent	Rotating with high frequency
Red Team	None	None	None	Red team	Red Team & Resilience Testing	Red Team & Resilience Testing
Purple Team	None	None	None	None	Purple Team	Purple Team
Application Testing	None	None	None	Basic	Dynamic (DAST)	Continuous (DAST)
Threat Assessment	None	None	None	None	Physical location assessment	Full threat assessment
Compromise Assessment	None	None	None	None	Compromise assessment	Compromise assessment

Increasing Frequency

Intensifying Scope

Off the Wheel…Next Steps

- Consider the cost benefit analysis
  - Testing expense
  - Remediation time
  - Training value
- Plan for the results

Off the Wheel…Next Steps

Evaluate your future testing strategy

- Understanding threat vectors/actors
- Variation of types
- Various channels
- Scope of work
- Frequency
- Using tests to train teams