Security Risk Management Process

Bruce Watson
Director, Office of Security and Emergency Management
WAPA Technology and Security Symposium, August 21, 2018
Security Risk Management Process

Risk = Function(Threats, Vulnerabilities, Consequences)

- Assess Assets
- Assess Threats
- Assess Vulnerabilities
- Assess Risk
- Determine Countermeasure Options
- Risk Decision

Risk Assessment (Baseline)/PSRA (Reoccurring)

Risk Decisions (Baseline)/PSRP (Reoccurring)

Formal Recurring Process Cycle that is Documented (i.e. PSRAs/PSRPs)
Process also includes Requirements Development

- ID Assets
- ID Undesirable Events
- How Undesirable Events are Achieved
- Value/Prioritize
- Need mission/risk owners
- Compliance vs. Real World
- What can be exploited?
- Threats: Attractiveness
- Several Different Methodologies
- Need mission owner/operators

DBT
Local Threats
Is there Residual Risk?
Is Residual Risk acceptable?

Mitigation Options:
- TTPs, Sec. Eng., Tech., Staffing, etc.
- Cost vs. Benefit

Accomplished at the Appropriate Level of Risk Acceptance