



Economics of Cybersecurity

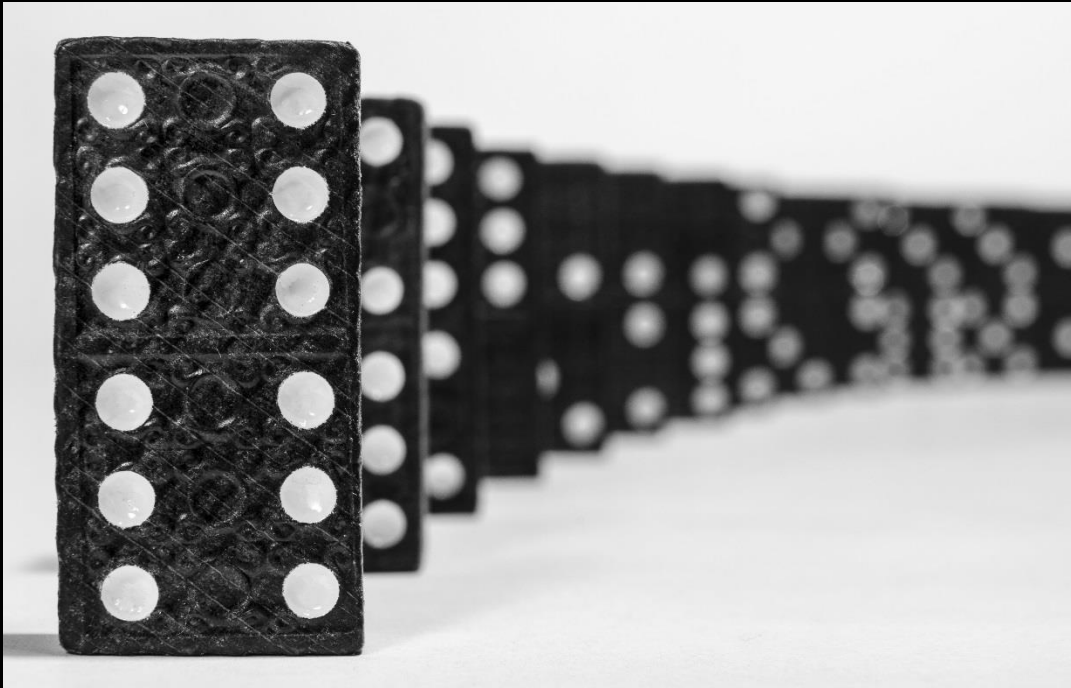
Paul Nielsen
Director and CEO
Software Engineering Institute
nielsen@sei.cmu.edu



How do you move the asymmetric imbalance?



Adopt a Risk Management Approach



- Assess critical assets
- Identify and assess threats and vulnerabilities to those assets
- Develop security policies and practices based on assessment

Focus on Resilience



Revise system and network architectures to reduce attack surface for critical assets

Treat security as a first-class requirement in acquisition and development

Continuously monitor networks and systems

Limit Damage/Reduce Recovery Costs



- Use pre-established response processes
- Plug into information resources that alert you to newly discovered vulnerabilities
- Train all employees to understand their security roles and responsibilities
- Capture lessons learned to refine policies and practices

What are the inhibitors to gaining asymmetric advantage?



SEI Experience Identifies Two Main Inhibitors



Failure to control system and network configuration

Failure to treat cybersecurity as a early design requirement

How do you measure
ROI on resilience vs.
security?



Gauge ROI According to Effect on Disruption



ROI on resilience addresses ability of organization to operate during and after disruption

ROI on security addresses organization's ability to prevent a disruption from occurring

