Homeland Security

Science and Technology

Cyber Risk Economics Capability Gaps Research Strategy

Erin Kenneally, M.F.S., J.D.
Cyber Security Division
Erin.Kenneally@HQ.DHS.Gov

Lucien Randazzese
SRI International
Lucien.Randazzese@SRI.com

CYRIE Program Overview

The Department of Homeland Security Science and Technology Directorate (DHS S&T) **Cyber Risk Economics (CYRIE)** program supports coordination and research into the business, legal, technical, and behavioral aspects of cyber risk economics relative to cyber threats, vulnerabilities, attacks, and controls.

Objectives

- Multi-Disciplinary
- Multi-Dimensional
- Value-Based for the Homeland Security Enterprise

Needs

- Prioritized Capabilities Gap Analysis & Needs Assessment
  - Investment
  - Impact
  - Value
  - Incentives

Execution

- Convene and Coordinate Stakeholders
- **Develop Knowledge Products**
- Fund Applied Research & Advanced Development

CYRIE Program Products

Coordinate & Convene

- Stakeholders: U.S. government officials, industry, researchers
- February 2017 Stakeholder Exchange Meeting (SEM) 1.0
  - Addressed capability gaps, practices, economic behavior, and research challenges
- September 2017 SEM 2.0
  - Addressed targeted capability gaps and research objectives

Knowledge Products

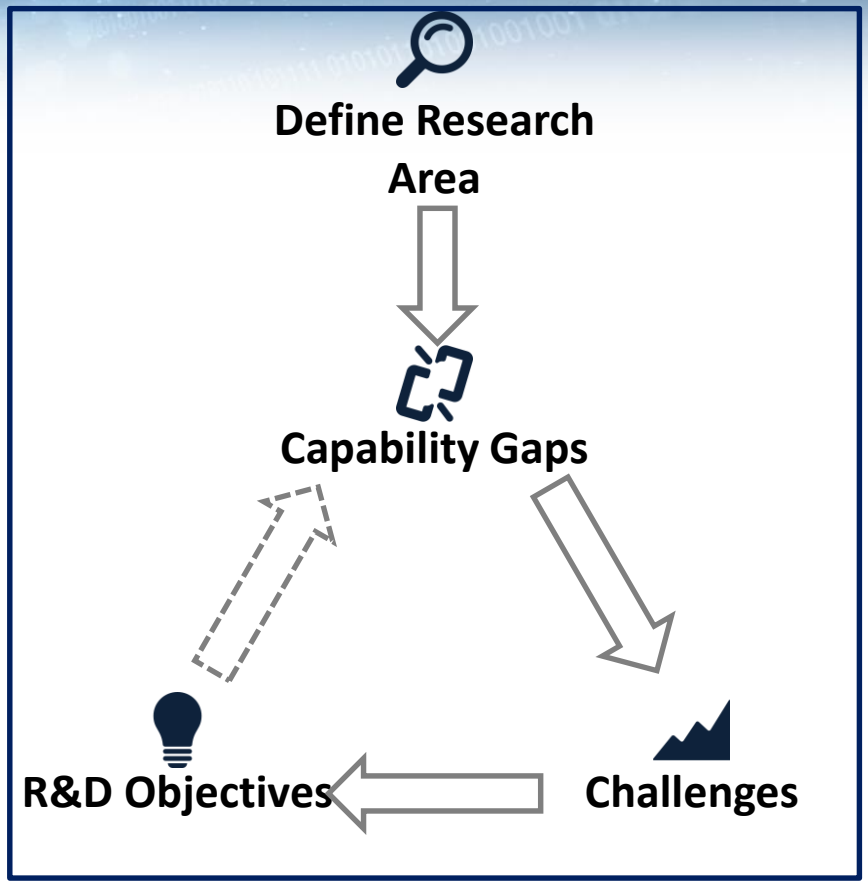
- Cyber Security Economics Research Literature Review
- **CYRIE Capability Gaps Paper (forthcoming)**

Applied Research & Advanced Development

- DHS S&T funds applied research and advanced development to enhance the security and resilience of the United States' critical information infrastructure and the Internet

Research Area Deep Dives

Research Areas
THEME 1 – The Quantification of Risk
Area 1 – Entity Risk Assessment
Area 2 – Systemic Risk Assessment
Area 3 – Impact of Controls
Area 4 – Decision Support
THEME 2 – Role of Government, Law, and Insurance
Area 5 – Role of Government Regulation
Area 6 – Role of insurance
Area 7 – Role of Law and Liability
THEME 3 – Third Party Risk
Area 8 – Supply Chain Accountability
THEME 4 – Organizational Behavior and Incentives
Area 9 – Organizational Effectiveness
THEME 5 – Data Collection and Sharing
Area 10 – Information Asymmetries
Area 11 – Data Collection and Mapping
THEME 6 – Threat Dynamics
Area 12 – Adversary Behavior and Ecosystem



Cyber Risk Economics – State of the Affairs?

THEME 1 – The Quantification of Risk

Area 1 – Entity Risk Assessment

- Measure the nature, size, frequency, and consequences of cyber-risks at the entity level
- Lack of understanding and incomplete assessment of cyber risks
- Difficulty to measure sources of cyber risk (especially hidden sources) and poor incentives
- Representative Research Objective: Develop prescriptive and flexible organizational-level cyber risk management models

Area 2 – Systemic Risk Assessment

- Measure the nature, size, and frequency of cyber risks in the ecosystem, including correlated and interdependent risk
- Ineffective and uncoordinated application of cybersecurity resources
- Data sources are not comprehensive and often not comparable
- Representative Research Objective: Develop models that improve the ability to describe complex systems with more precision and enhance the quality and fidelity of risk assessments for decision makers

THEME 1 – The Quantification of Risk

Area 3 – Impact of Controls

- Evaluate how investment in controls changes risk and outcomes
- Deficient understanding of how investment in controls changes their risk levels, making it difficult to choose the appropriate level of investment
- Risk and control implementation relationship is complex, and data is scarce (especially ex-ante data)
- Representative Research Objective: Quantify how investments in specific controls change risk and outcomes

Area 4 – Decision Support

- Understand and improve control investment decision making
- Traditional investment decision tools are of limited use for cybersecurity risk management, and frameworks can lead to a check-box mentality
- Widespread standard framework adoption is relatively recent across a wide variety of organizational vulnerability and threat profiles
- Representative Research Objective: Evaluate framework effectiveness in supporting decision making, including any systematic gaps or biases in controls investment that may result from their use

THEME 2 – Role of Government, Law, & Insurance

Area 5 – Role of Government Regulation

- Assess the impact of cybersecurity regulation on cyber risk and outcomes
- Economic effects models are largely theoretical, and policy is focused on consumer protection
- Regulations are difficult to influence, forecast, and model comprehensively
- Representative Research Objective: Identify the conditions when government should act as coordinator and facilitator of industry-driven processes vs. those under which it should act as a top-down regulator of requirements

Area 6 – Role of Insurance

- Understand the effects of insurance on cybersecurity investment and cyber risk and outcomes
- Risk quantification and cyber insurance benefits are not well understood
- Correlated and interdependent risks make analysis difficult
- Representative Research Objective: Quantify the ecosystems-wide effect of insurance on risk exposure and resiliency

Area 7 – Role of Law and Liability

- Understand the role of law and liability in cyber risk outcomes
- Cybersecurity standard are uncertain and cyber liability case law is inconsistent
- Harmful disclosure and use of information can be difficult to evidence
- Representative Research Objective: Study how existing product liability frameworks may be applied to address cybersecurity failures in the context of increasingly connected networks and devices

THEME 3 – Third Party Risk

Area 8 – Supply Chain Accountability

- Approaches for improving accountability for security within complex supply chains
- Component and system manufacturers lack techniques and legal/regulatory frameworks to account for cyber risks induced by third party-supplied technologies
- Complexity and interconnectedness of systems, diversity of vendors, price-based competition, unclear legal frameworks
- Representative Research Objective: Model incentives and mechanisms for up- and downstream suppliers (devices, applications, platforms, networks, services) to cooperate to improve cybersecurity

Who should bear the costs imposed by insecure devices?

THEME 4 – Organizational Behavior & Incentives

Area 9 – Organizational Effectiveness

- Evaluation of the organizational characteristics associated with effective cybersecurity
- Diversity in hard control implementation, endogenous vulnerabilities, and exogenous factors (dynamic actions of attackers)
- Difficult to isolate hard control effects from organizational culture and soft control effects
- Representative Research Objective: Develop models for integrated cybersecurity expenditures by organizations – where spending for cyber insurance for risk transfer risk can be considered and balanced with other aspects of cybersecurity behavior such as avoidance, acceptance, and mitigation in order to optimize risk management strategy

The role of organizational attributes related to culture and management is an underestimated factor

THEME 5 – Data Collection & Sharing

Area 10 – Information Asymmetries

- Identify how information deficiencies and asymmetries in the ecosystem affect risk, behavior, decisions, and outcomes
- Lack of understanding and incomplete assessment of cyber risks
- Difficulty isolating, measuring, and analyzing real world scenarios
- Representative Research Objective: Examine new techniques and underlying assumptions for empirically-based analysis

Area 11 – Data Collection & Mapping

- Development of tools for efficient and systematic collection of cyber environmental data, and correlation/translation to business-centric data and metrics
- Limited data availability due to significant capability gaps
- Data sharing disincentives, lack of sharing incentives, data access limitations, lack of shared definitions
- Representative Research Objective: Collect, map, and analyze data assets to generate multi-stakeholder sharing mechanisms

THEME 6 – Threat Dynamics

Area 12 – Adversary Behavior & Ecosystem

- Understand the behavior and decision making of attackers
- Lack of knowledge about attacker processes, incentives, and strategies to inform more effective defense tactics
- Issues distinguishing the motivations and strategies behind adversary behavior, especially given the hidden nature of attacks and attackers
- Representative Research Objective: Identify and establish metrics for evaluating and impeding cyber criminals

Effective defense requires knowledge of attacker processes, incentives, and strategies