Homeland Security

Science and Technology

CyRiE

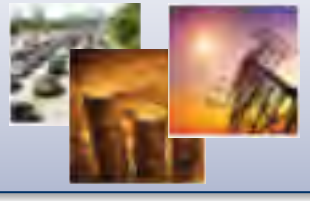
Cyber Risk Economics

Erin Kenneally, M.F.S., J.D.
Program Manager
Cyber Security Division

CSD Mission & Strategy

REQUIREMENTS





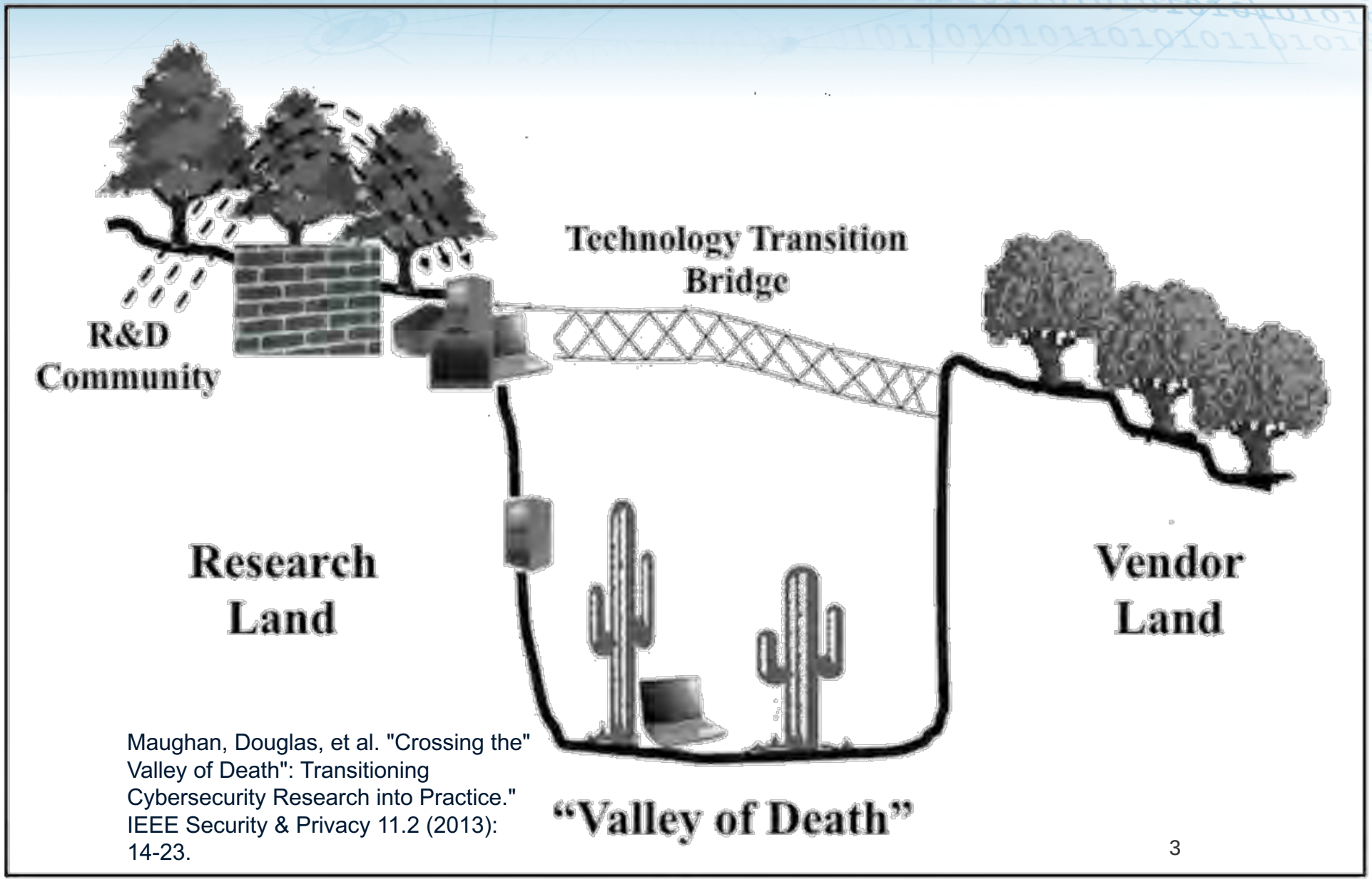
MISSION

- **Develop and deliver new technologies, tools and techniques** to defend and secure current and future systems and networks
- Conduct and support **technology transition** efforts
- Provide **R&D leadership and coordination** within the government, academia, private sector and international cybersecurity community

PROGRAMS

- **Cyber for Critical Infrastructure**
- **Cyber Security for Law Enforcement**
- **Cybersecurity Outreach**
- **Cyber Physical Systems**
- **Data Privacy Technologies**
- **Identity Management**
- **Homeland Security Open Source Technologies**
- **Human Aspects of Cyber Security**
- **Mobile Security**
- **Next Generation Cyber Infrastructure Apex**
- **Network System Security**
- **Research Infrastructure**
- **Software Assurance**
- **Transition to Practice**

Valley of Death Between Research & Industry



Maughan, Douglas, et al. "Crossing the" Valley of Death": Transitioning Cybersecurity Research into Practice." IEEE Security & Privacy 11.2 (2013): 14-23.

Cyber Risk Economics: So Many Q's, So Few A's

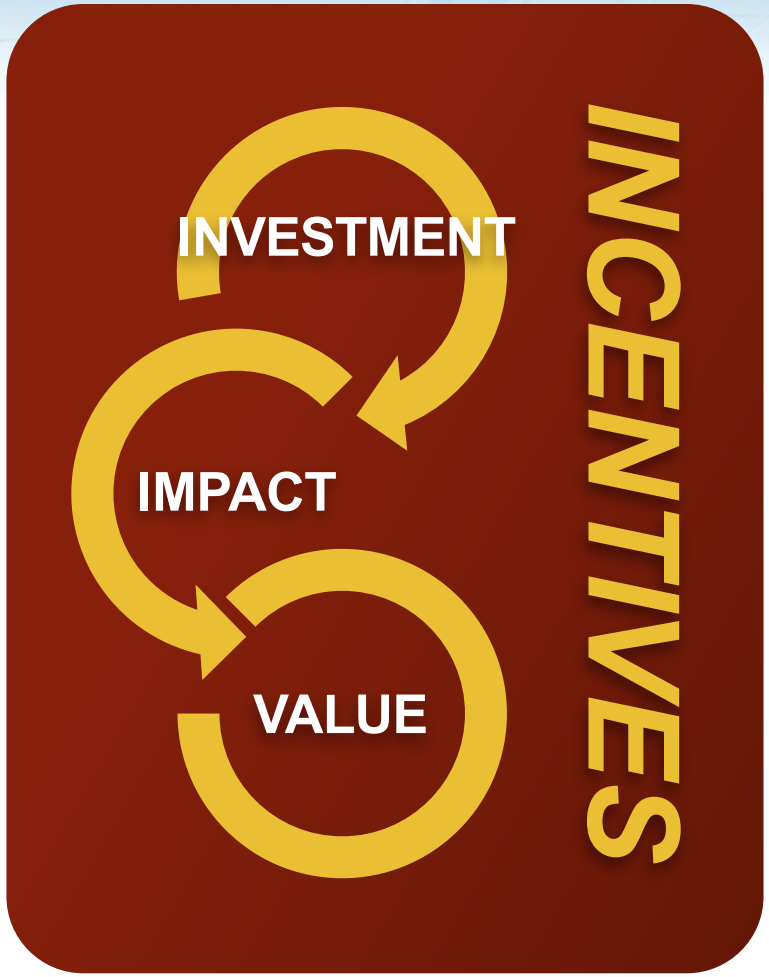
- What drives current investment levels? I.e., what are the relative contributions of: liability protection; need to offset the direct financial costs of breaches; fear of the impact of reputational damage?
- Can/How should organizations measure the benefits of avoided incidents?
- What would incent firms to place more value on the impact of breaches borne by other entities (e.g. business partners, customers, etc.)?
- How does the magnitude of "targeted damage" compare to "collateral damage?"
  - I.e., what is the size of the externality impact versus direct organizational impact of a breach?
- How does the magnitude of cyber risk associated with attacks on physical infrastructure compare to the magnitude of the cyber risk associated with breached data?
- Where, in the distribution of assets and organizations, is the largest risk currently present?
  - organization type, size, location, sector, asset/activity type?
- Under what circumstances is regulation more/less effective in incenting better cybersecurity behavior?
- How does the effectiveness of framework-based cybersecurity decision-making compare to those based on other decision methods?
- Should we focus on sharing actual experience with specific cyber security controls, measures and effectiveness?
  - Would this help overcome a potential CISO view of the security market as a market for lemons?
- How can understanding the Tactics, Techniques and Procedures (TTPs) of attackers be used to identify the type of controls required to defend against them?

Enter CyRiE

- **OBJECTIVE**:
  - enhance solutions (metrics, measurement, modeling) addressing the business, legal, technical, and behavioral aspects of the economics of cyber threats, vulnerabilities, and controls.
- **WHO**:
  - improve value-based decision making by those who own, operate, protect, and regulate the nation's vital data assets and critical infrastructure.
- **WHAT**:
  - beyond the traditional economic-based view of incentives for cybersecurity
  - cybersecurity risk as a multidimensional problem that requires multidisciplinary perspectives

Homeland Security
Science and Technology

Program Strategy (Cont'd)



- **HOW**: CyRiE executes its vision along four related dimensions
  - **Investment**: How and why are cybersecurity investments made?
  - **Impact**: What impact do cybersecurity investments have on risk and harm?
  - **Value**: Relationship between cybersecurity risk and traditional business risk?
  - **Incentives**: What are needed to encourage optimal cyber risk management?
- **Knowledge Products, Technology, and Coordination**

Homeland Security
Science and Technology

Capability Needs & Gaps

- Derived from a number of authoritative policy documents:
  - **DHS Cybersecurity Incentives Study** – June 2013, response to Executive Order 13636, Improving Critical Infrastructure Cybersecurity
  - **Cybersecurity Game-Change R&D Recommendations** – May 2010, Networking and Information Technology Research and Development (NITRD)
  - **Federal Cybersecurity Research and Development Strategic Plan** – February 2016, National Science and Technology Council
  - **Presidential Policy Directive 21** – PPD on Critical Infrastructure Security and Resilience, February 2013
  - **Executive Order 13718** – Commission on Enhancing National Cybersecurity, February 2016.
  - **National Privacy Research Strategy** – June 2016, Obama Administration, National Science and Technology Council

(1) Operationalizing the Vision: Coordination

- **Initial Stakeholder Engagement: Stakeholder Exchange Meeting (SEM)** (Feb '17)
- Brought together **key stakeholders**:
  USG officials, Industry, Researchers
- **Goal**: capability gaps, practices/behavior/beliefs, and research challenges relating to Investment, Impact, Value and Incentives

- **USG stakeholder-customers** include: Department of Commerce (NIST, NTIA); Department of Homeland Security (NPPD, OSIA, CS&C, CIDAR Project), Department of Defense (DARPA), Federal Communications Commission (Cybersecurity and Communications Reliability), Health and Human Services (Critical Infrastructure Protection Branch), National Science Foundation (SATC), Department of Treasury (Office of Critical Infrastructure Protection and Compliance Policy), General Services Administration, Executive Office of the President (OSTP), Consumer Financial Protection Bureau, Securities and Exchange Commission, and Commodity Futures Trading Commission.

(2) Operationalizing the Vision: Knowledge Products & Technology areas

- Empirical data on the **relative value of cybersecurity controls**
- Modeling economic **value of information harvested in breaches/attacks** and correlation with variables such as industry sector, corporate security practice
- Methods and tools to **understand cyber criminal ecosystem** at the macro-level (responses to takedowns, scams or other adversarial behavior) and micro-level (tracking underground vendor strategies, mergers, etc.)
- Metrics and data for incident forecasting and risk profiling for **cyber insurance modeling of dependencies and aggregation**
- Model **how human cognitive biases affect cyber security professionals and executives** in assessing cyber risk and subsequent actions

e.g., CyRiE R&D

Identifying How Firms Manage Cybersecurity Investment

Tyler Moore
Tandy School of Computer Science
University of Tulsa, USA
tyler-moore@utulsa.edu

Scott Dynes Frederick R. Chang
Darwin Deason Institute for Cyber Security
Southern Methodist University, USA
{scottd,chang}@smu.edu

Abstract

We report on a set of 40 semi-structured interviews with information security executives and managers at a variety of firms and government agencies. The purpose of the interviews was to learn more about how organizations make cybersecurity investment decisions: how much support they receive to execute their mission, how they prioritize which threats to defend against, and how they choose between competing security controls. We find that most private sector executives believe that their firms adequately fund cybersecurity, but that finding qualified personnel inhibits the pace of adoption of new controls. Most firms do not calculate return on investment (ROI) or other outcome-based quantitative investment metrics; instead, they opt for process-based frameworks such as NIST and COBIT to guide strategic investment decisions. Finally, we note that CISOs in government face considerable challenges compared to their private-sector counterparts.

Ex. (1) R&D: How Do Firms Manage Cybersecurity Investment (Moore, U. Tulsa)

Do organizations calculate ROI to make investment decisions?

- Some firms use quantitative metrics to measure and improve operational security: counting # unpatched machines, # malware infections remediated, etc.
- Almost nobody used quantitative metrics to guide *investment* decisions
  - Exception: minority translated budget requests into ROI, but still expressed skepticism that these were important in driving any decision
  - One CISO stated he doesn't want to sell security to the board by saying "there's a 20% chance of a $20 million breach in a given 5 years"; argument doesn't resonate
  - Healthcare CISO: "in security, ROI is a fallacy. We are a cost center"

THE UNIVERSITY of TULSA

T. Moore, S. Dynes and F. Chang. Identifying how firms manage cybersecurity investment. In Workshop on The Economics of Information Security, 2016. http://tylermoore.ens.utulsa.edu/weis16ciso.pdf

Ex. (2) R&D: Understanding and Disrupting the Economics of Cybercrime (Christin, Carnegie Mellon U)

- Cyber-security attacks cost money
  - Estimates vary and are highly disputed, but:
  - A couple of hundreds of millions of dollars per year in **direct costs** to victims
- **Indirect costs** (policing, etc) are extremely high!

Criminal revenue	Cost in policing
Large botnet: **1/3 of the spam on the Internet** Made its owners **2.7 million USD** in a year	How much did we invest in email spam reduction over that year? **> 1 Billion USD**

- Can we be smarter? How?
  - Focusing limited law enforcement resources on the points where they matter the most

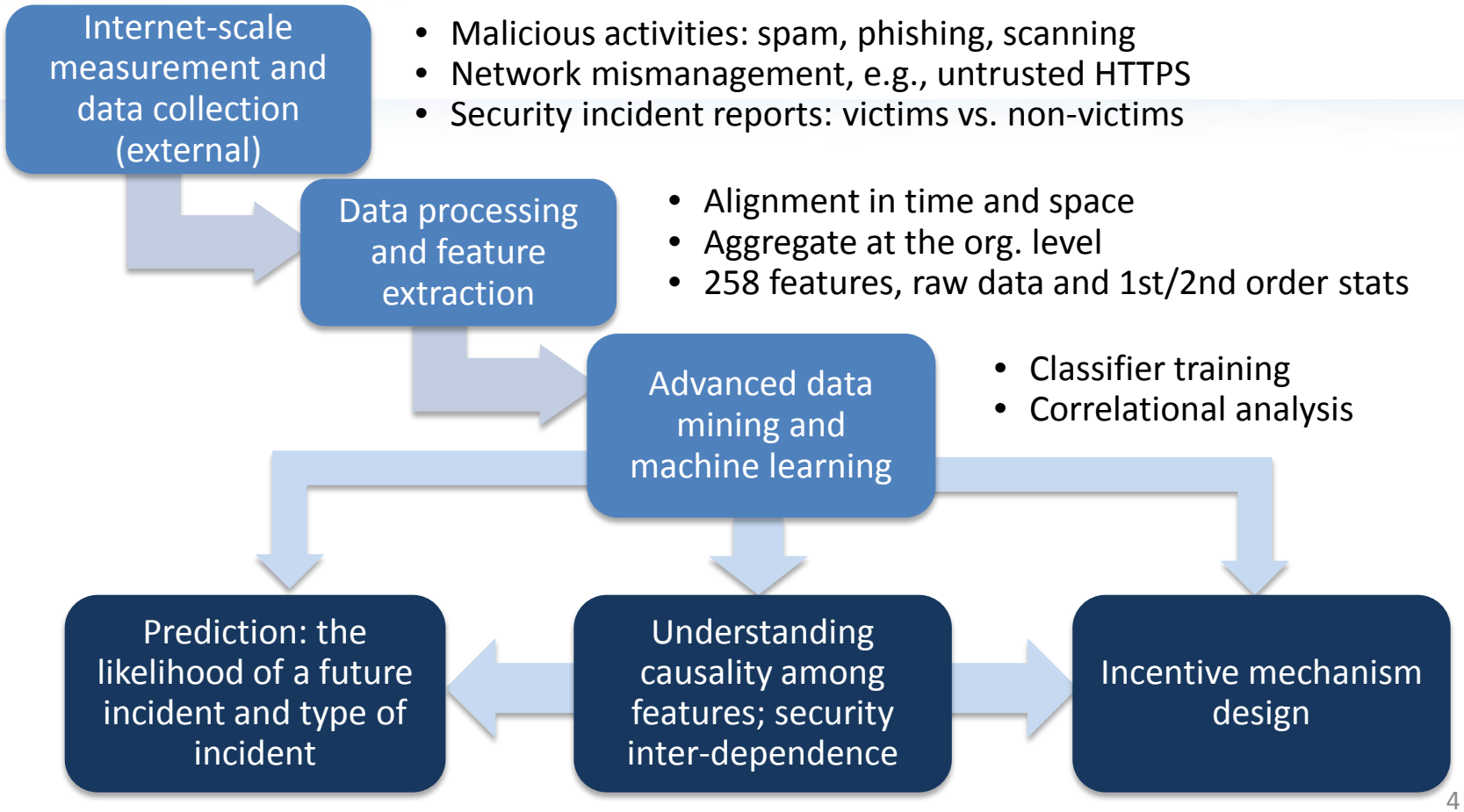
(con't, Christin CMU)

- Criminals are mostly in it for the money
  - Do cost/benefit analysis too!
- **Very** economically rational
  - **Will** give up if costs become too high
    - "Visa is burning us with napalm" (some illicit Rx seller on the Internet)
    - "Will close shop until Bitcoin value stabilizes" (a drug dealer on the Silk Road anonymous marketplace)

1) Need to adopt a **data-driven** approach—and avail data
2) Need to find and exploit **concentration** points (that can lead to effective financial pressure on criminals
3) Need to understand why victims fall for attacks, what are defenses deemed acceptable by the public

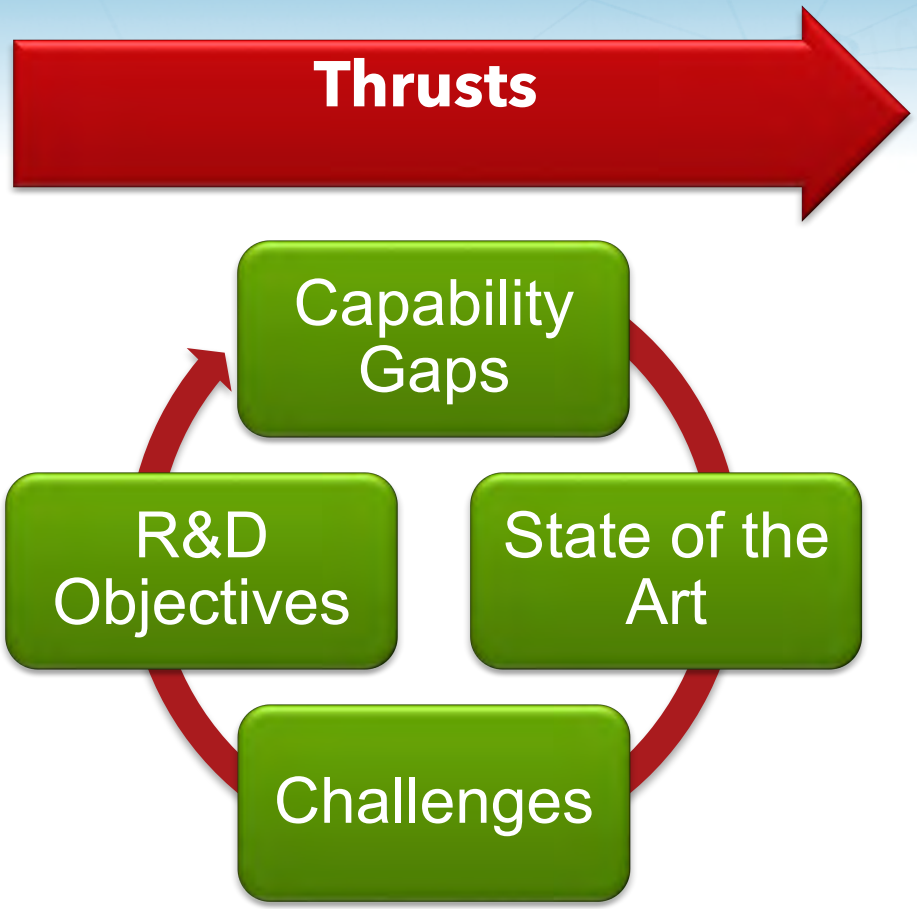
Network measurements + economic and behavioral analysis

e.g., (3) R&D: Measuring Cyber Risk (Liu, U Michigan)



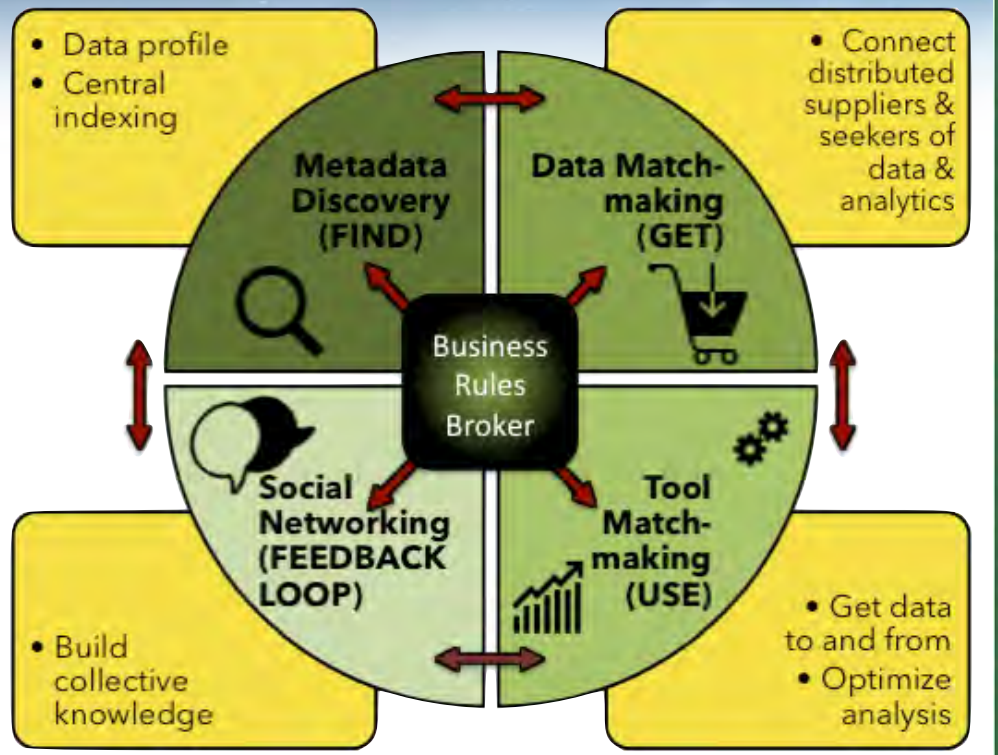
- Building a Global Network Reputation System: Metrics, Data Analysis, and Risk Prediction, U. of Michigan Mingyan Liu

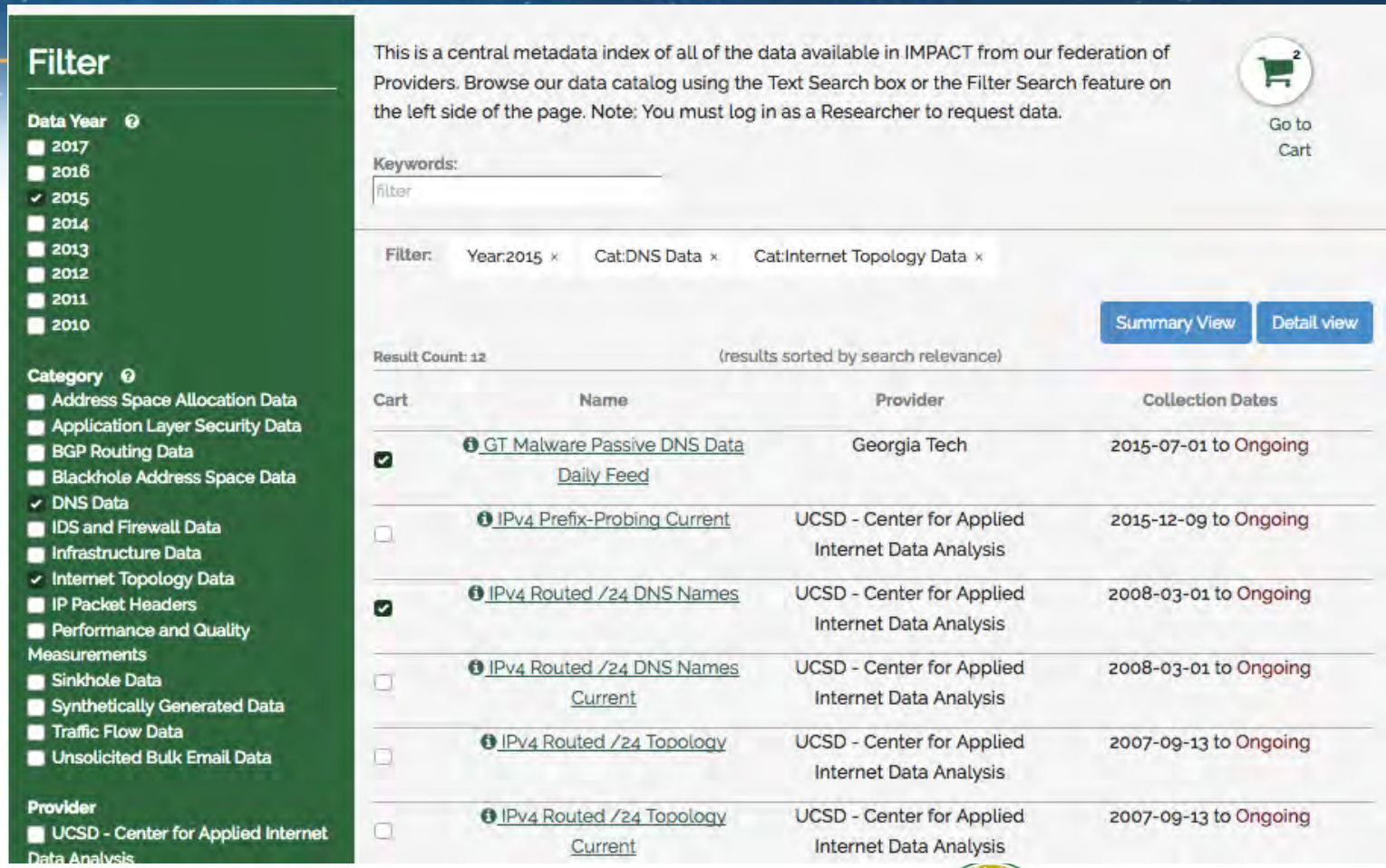
(3) Operationalizing the Vision: CyRiE R&D Green Paper



- **Quantification of Risk:**
  - **Decision Support:** the effect of decision frameworks use on impact and investment
  - **Impact Assessment:** nature, size, frequency, and effect of cyber-risks faced by different entities
  - **Controls Investment:** relationship between investment and risk to potentially impacted parties
- **Role of Gov't, Regulation, Policy**
  - What is the impact of cybersecurity regulation on outcomes
  - How can the government balance accountability, transparency, data sensitivity in reporting?
- **Role of Insurance**
  - What are the effects of insurance on cyber risk impact and cyber security investment? Do they have a positive impact? How to improve with cyber environmental data?
- **Role of Law & Liability**
  - Understanding of how exposure to liability changes behavior, investment, and outcomes
  - Assess & assign accountability within and across supply chains
- **Organizational Behavior & Incentives**
  - What are the org characteristics associated with effective cyber security?
  - Comparative effectiveness of mandatory cyber insurance, tax subsidies, standards for self-protection
- **Data Collection & Sharing**
  - Identifying and correcting information asymmetries
  - tools for efficient and systematic collection of cyber environmental data and correlation/translation to business-centric data and metrics
- **Threat Dynamics**
  - Adversary Behavior: Understanding the behavior, adaption, and decision-making
  - Adversary Ecosystem: Understanding of group behavior and macro economics of attacker platforms; intervention points

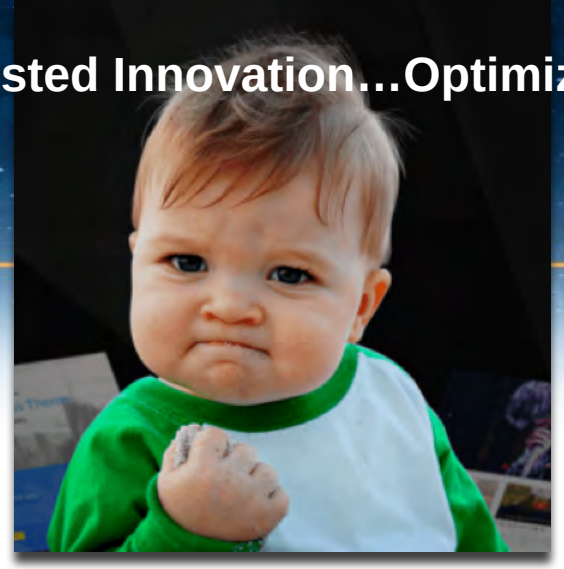
IMPACT: Information Marketplace for Policy and Analysis of Cyber-risk & Trust





www.ImpactCyberTrust.org

Trusted Innovation…Optimized.



Erin Kenneally, M.F.S., J.D.
Program Manager
Cyber Security Division
Science & Technology Directorate
Dept of Homeland Security
Erin.Kenneally@HQ.DHS.Gov

Homeland Security
Science and Technology

CYRIE
CYBER RISK ECONOMICS
INVESTMENT
IMPACT
INCENTIVES
VALUE