Cyber Risk Economics Capability Gaps Research Strategy

Erin Kenneally
U.S. Department of Homeland Security
Cyber Security Division
International Computer Sciences Institute
Washington, DC USA
erink@icsi.berkeley.edu

Lucien Randazzese
SRI International

Arlington, VA USA
lucien.randazzese@sri.com

David Balenson
SRI International

Arlington, VA USA
david.balenson@sri.com

***Abstract*—This paper calls attention to a forthcoming publication produced by the Cyber Risk Economics Program within the U.S. Department of Homeland Security. It presents an overarching strategy for cyber security risk economics applied research and advanced development intended to address some of the most pressing capability gaps in government and industry.**

Keywords—risk, economics, cyber security, insurance, data sharing, incentives

I. INTRODUCTION

Cybersecurity is a multidimensional problem that demands multidisciplinary attention. The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Risk Economics (CYRIE) program supports research into the business, legal, technical and behavioral aspects of the economics of cyber threats, vulnerabilities and controls.[1]

The CYRIE program has developed a forthcoming Green Paper that frames a series of research areas derived from capability gaps drawn from a confluence of authoritative documents, scholarly literature review and a range of recent stakeholder discussions of cyber-risk economics. These areas comprise many of the hardest problems in this field and thus problems against which progress is expected to translate to improved cyber-risk management. The paper's objective is to frame a research agenda to close the gap between research and practice, by apprising the research community of real-world cyber risk economics challenges, and, ultimately, to inform evidence-based policy and actions by industry and government organizations. The expected output from research in these areas contemplates the creation of new and improved data, measurements, models and metrics.

In 2013 two executive actions were issued, aimed at enhancing the capability of owners and operators of the nation's critical infrastructure to protect their networks and systems against cyberattack (Executive Order 13636, Improving Critical Infrastructure Cybersecurity[1] and Presidential Policy Directive 21, Critical Infrastructure Security and Resilience[2]).

[1] Department of Homeland Security, Science and Technology Directorate, Cyber Security Division, Cyber Risk Economics (CYRIE). https://www.dhs.gov/science-and-technology/csd-cyrie.

These authoritative policy documents gave DHS a coordinating role in pursing the cybersecurity objectives outlined in each and directed the National Institute of Standards and Technology (NIST) to develop a voluntary framework that owner/operators could use to improve their cybersecurity posture. DHS led an interagency working group focused on cyber-economic incentives and together with the departments of Commerce and Treasury prepared an analysis of federal policy options for incenting adoption of the NIST framework. DHS S&T continues to maintain active engagement in the effort to understand and develop stronger cybereconomic incentives, through its R&D efforts and portfolio.

The working group and the resulting analysis focused primarily on policy and incentives from a microeconomic-based view of the marginal costs and benefits of adoption. While this analysis provided a solid start for the study of incentives in cybersecurity, it also showed that a more holistic approach to research in the area of cyber risk economics was clearly needed, one that incorporates perspectives on security decisions and behavior from a wide range of social and behavioral sciences.

II. PURPOSE AND APPROACH

The CYRIE program endeavors to improve value-based decision-making by those who own, operate, protect and regulate the nation's vital data assets and critical infrastructure. As such, the program looks beyond the traditional economics view of incentives for cybersecurity – where individuals are assumed to be rational actors who know how to maximize their well-being – and considers a broader array of factors that include business, legal and behavioral economics. In this way, CYRIE research and development (R&D) can more effectively address strategy and tactics for optimal cyber-risk avoidance, acceptance, mitigation and transfer.

CYRIE R&D emphasizes the empirically based measurement, modeling and evaluation of four related dimensions:

- **Investment** – how and why individuals and organizations invest in controls to manage cyber risk;
- **Impact** – what impact do investments have on risk and outcomes to information, systems and people;

Presented at 2018 International Workshop on Cyber Insurance and Risk Controls (CIRC), held in conjunction with the IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA 2018), June 11-12, 2018, Glasgow, Scotland, UK. To be published by IEEE.

- **Value** – what is the relationship between cybersecurity risk and conventional business performance and financial frameworks that guide decisions; and
- **Incentives** – what incentives are needed to encourage effective cyber risk management.

Figure 1: CYRIE Program Focus Areas

Recognizing the importance of data sharing to building capacity across these four dimensions, CYRIE supports the sharing of cybersecurity best practices, investments, incidents and outcomes among diverse stakeholders. For example, from an operational standpoint, data exchanges can be valuable in addressing the technical aspects of risk economics in situations where risks evolve more quickly and spread more widely than defensive controls. Value-based risk management of the shared environments that challenge cybersecurity demands more collective information. Effective information sharing can help mitigate against the often-siloed view of risk, create positive network effects and foster exponentially increasing "Return on Sharing" or "ROS."

As well, CYRIE supports the development and operationalization of technical and knowledge solutions to help organizations address the specific cyber-risks they face. The program also aims to inform the government about how it can reduce cyber risk levels through development and enforcement of policy and regulation, convening and coordination of stakeholders, adoption of technology, promulgation of standards, and facilitation of research and development.

Three broad categories of input were used to guide the formulation of the research areas proposed in the forthcoming paper:

1. Insight and ground truth gleaned from several 2017 Stakeholder Exchange Meetings (SEMs) on cyber-risk economics research, stewarded by the Cyber Security Division within the DHS S&T. The meetings brought together key stakeholders- leaders, technologists and researchers- from government, industry and academia to discuss capability gaps and needs relating to the business, legal, technical and behavioral aspects of cyber threats, vulnerabilities and controls.
2. A comprehensive review of academic research in cyber risk economics identified the state of art of CYRIE research.
3. A collection of principal U.S. federal government documents covering cybersecurity incentives provided essential context about the needs and goals of federal entities, including Presidential Policy Directives, Executive Orders and the Federal Cybersecurity R&D Strategic Plan[3].

III. Research Themes and Areas

The Green Paper[2] describes 12 research areas organized into 6 themes:

THEME A – The Quantification of Risk
Area 1 – Entity Risk Assessment Area 2 – Systemic Risk Assessment Area 3 – Impact of Controls Area 4 – Decision Support
THEME B – 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 C – Third Party Risk
Area 8 – Accountability within Complex Supply Chains
THEME D – Organizational Effectiveness
Area 9 – Organizational Behavior and Incentives
THEME E – Data Collection and Sharing
Area 10 – Information Asymmetries Area 11 – Data Collection and Mapping
THEME F – Threat Dynamics
Area 12 – Adversary Behavior and Ecosystem

Figure 2: Proposed Cyber Risk Economics Research Areas

Each research area is framed as follows, with some overlap due to the related nature of the topics:

- Current gaps in capability or understanding
- Known or expected solution challenges
- Key research objectives

Below is a very abbreviated selection of content contained therein.

A. Quantification of Risk

The inability of organizations to understand and assess the cyber risks they face individually and collectively remains a fundamental challenge in cybersecurity. As early

[2] The Green Paper is currently in unofficial DRAFT version: PLEASE DO NOT CITE WITHOUT PERMISSION; please contact one of the authors for pointer to the forthcoming, final published version of the Green Paper including the formal citation.

as 2003[4], the Computer Research Association identified the development of "accurate risk analysis for cybersecurity" as one of four trustworthy computing grand challenges and attributed a large share of the blame for low information security spending to lack of effective models of risk.

Developing effective, quantitative risk-management data, models and metrics is made challenging by the inherently hard-to-measure and hidden nature of most sources of cyber-risk, be they attackers, insider threats or the poor cybersecurity practice of partner organizations. Poor incentives exacerbate the problem. Most organizations at risk are also not incented to disclose vulnerability and attack data and the significant variation in risk levels across organizations and organizational types challenges the notion that cybersecurity risk is a homogeneous problem.

Recent research and market attempts to characterize and predict firm-level security risk using publically available network data show promise that quantification challenges can be overcome[5][6]. A key challenge to more accurate and complete risk understanding is accumulating risk measures inside the firm and correlating these with externally-facing risk data and with actual loss event data. We know from practice that cyber-risk is not independent and is highly correlated across entities in an ecosystem, but we have a limited understanding of the correlation of risk across the system, and an imperfect view of where risk is concentrated.

Much current knowledge of risk is derived from estimates of breach frequency and impact from surveys or analyses of aggregated data with wide variance in the size, frequency and severity of risk, suggesting fundamental data inadequacy across the board.

As well, organizations have an imperfect understanding of how investment in controls changes their risk levels, making it difficult to determine the optimal or even effective levels of investment. Even when security standards can be established, they cannot be predictably mapped to measurable controls. At the same time, there is little agreement on metrics and measurement of harm. The correlation between risk and controls is difficult to analyze because the relationship is complex and mediated by numerous, hard-to-measure endogenous and exogenous variables.

Finally, organizations find traditional financial investment decision tools to be of limited use for cybersecurity. Most organizations rely instead on frameworks[7], which provide for good functional disaggregation (e.g., Identify, Protect, Detect, Respond and Recover), but do not provide as much guidance on what investments are needed to reduce risk. When cyber-risk metrics are collected and reported they are often framed in qualitative or operational terms (e.g., number and timeliness of systems patched) but are rarely quantified using traditional financial measures that guide investment decisions in other areas of risk, such as ROI. As a result, cyber risks are less likely to receive necessary attention and resources.

Examples of research objectives across this theme are:

- Understand the key attributes around which risk (nature, severity and probability) is distributed, such as third-party relationships, customer base size, type of information stewarded, and online footprint
- Develop tools and mechanisms to effectively communicate cyber-risk to executive and other non-technical audiences for decision support
- Characterize risk distribution across various ecosystems
- Develop and validate metrics and measures of the degree, effect and location of correlated and concentrated risk
- Build models to relate system-level risk to organizational-level risk and ecosystem-level risk
- Collect historical data and develop analytic models to predict system conditions after the occurrence of a high-consequence/low-probability event
- Develop analytics that identify and characterize security properties of connections between networks and systems, e.g., identify and characterize relationship between security properties along the OSI stack, network mapping and inter-domain internet topology
- Develop value- and outcome-based measures and metrics for assessing efficacy of technical controls[3]
- Develop models, simulations and exercises that communicate the full range (direct and indirect) of the impacts of cyber incidents
- Develop hybrid approaches that integrate process-driven framework models for cybersecurity decision making

B. Role of Government, Law and Insurance

The impact of regulation on risk and outcomes in cybersecurity is critically important but evaluation to date has been limited. This is due in part to poor insight and assessment of the behavioral and economic impact on asset owners, users and attackers, including impairment to innovation from increased compliance costs. In addition to gaps with respect to analysis of the role of regulation in cybersecurity, there are limitations with regulation itself, at least so far as industry perceives it. For example, there is a lack of models to help regulators balance tensions between accountability and transparency, e.g., requiring mandatory cybersecurity incident reporting while also considering legitimate data sensitivity concerns.

---

[3] The DHS S&T CYRIE program funded 418 Intelligence under the FourSight Platform for Crowdsourcing Cyber Security Controls project, Agreement Number FA8750-16-9-9000, https://www.dhs.gov/science-and-technology/news/2018/01/03/news-release-st-awards-350k-spur-cybersecurity-info-sharing.

Perhaps the biggest issue facing insurance markets is accurate risk quantification, which necessitates better data on cyber threats, vulnerabilities, attacks, and controls in order to advance insurance underwriting, risk control and policies[8]. On the underwriting side, lack of cybersecurity domain expertise and relevant actuarial information leads to policies that can be ill-fitting or over/under inclusive. The challenges to developing effective markets for cybersecurity insurance are well documented[9]. Correlated and interdependent risk make underwriting difficult as does the presence of downstream harms and liability risk.

In the United States, trends have arisen in the interpretation and application of laws and contracts that have diminished the role of liability as a forcing function on organizational behavior toward cyber risk. For example, courts addressing cases seeking legal recourse for cybersecurity and data breach events have largely dismissed them for failure to establish standing or prove cognizable damage and actionable harm.

Examples of research objectives across this theme are:

- Understand the circumstances under which regulation potentially degrades overall security practice and exacerbates systemic risk
- Develop comparative analysis and recommendations for proper application of incentives instruments such as public-sector procurement, tax, subsidies, liability or regulation
- Understand how availability and use of cyber insurance affects other aspects of cybersecurity behavior
- Create and prototype socio-technical mechanisms for accountable data sharing within the insurance industry
- Develop mechanisms for broader and more effective use of relevant environmental data in cyber insurance underwriting (e.g., technical and engineering data such as network asset and architecture data, security technologies and platforms in use, scope and nature of sensitive data, critical control systems in use, etc.)
- Develop metrics to assess the accuracy and reliability of cybersecurity risk rating techniques used by industry and adopted by insurance carriers in lieu of desired actuarial data
- Evaluate the potential effectiveness (fairness, deterrent effect) of transitive liability models on manufacturers, developers, integrators and other vendors of insecure devices/software
- Conduct a comparative study of how mandatory insurance coverage in other areas – workers comp, auto, homeowner, health – is responsible for volume and quality of data needed for actuarial and prediction and can be applied to cyber-risk data deficiency
- Develop accountability mechanisms for shared responsibility environments

C. Third Party Risk

There is growing support for the contention that supply chain actors – manufacturers, service providers and developers – should bear the costs imposed by insecure devices in order to ensure that vendors take adequate precautions to prevent broad-scale harm to Internet infrastructure. It can be quite challenging to assign responsibility in the context of systems comprised of devices and software from numerous vendors and assets inside and outside a breached organization's network.

The complexity and interconnectedness of IT networks and systems render the application of existing legal frameworks and development of new frameworks for liability inherently difficult. The scale and diversity of vendors, strong incentives to compete on price and not security, and lack of incentive to coordinate security and privacy efforts suggest, an impending market failure for security in IoT. As such, there is a need for new risk accountability solutions that combine market-based incentives and regulatory oversight (e.g., equipment certification, procurement standards and data flow transparency) to reduce cyber-risk.

Examples of research objectives across this theme are:

- Model incentives and mechanisms for up- and downstream suppliers (devices, applications, platforms, networks and services) to cooperate to improve cybersecurity
- Understand how exposure to liability in complex supply chains changes behavior, investment and outcomes
- Develop mechanisms to correct or mitigate information asymmetry faced by stakeholders in the supply chain; for example, a model bill of materials for IoT stakeholders or an audit capability to enable manufacturers to reliably certify the security of components when choosing among prospective suppliers

D. Organizational Behavior and Incentives

Organizations exhibit great variability in security posture. Much of the variance is owing to diversity in investment in hard controls, differences in endogenous vulnerabilities, and exogenous factors such as the dynamic actions of attackers. The role of organizational attributes related to culture and management is an underestimated factor.

Also in short supply are socio-technical models for identifying and correlating behavioral (individual, organizational and social), economic, and technical factors that can affect security performance. Further, there has been little attention paid to the role of cognitive biases in individual decision making by executives or security operations staff. Results from recent research on how cognitive biases affect cybersecurity professionals finds it to be potentially quite significant[10].

Examples of research objectives across this theme are:

- Map how incentives at the organizational level get translated to the level of individual behavior; and, identify individual incentives that lead to better organizational performance
- Identify the conditions for which automating decisions and actions (i.e., getting people out of the loop) are preferable and when they are not
- Investigate how the cognitive biases often associated with poor decision making can be exploited to improve behavior

E. Data Collection and Sharing

The effects of information shortfalls on risk, behavior, decisions and outcomes have been extensively considered in the research literature. For example, the security market is subject to inaccurate disclosure, by which organizations are incented to underreport damage from cyberattacks for reputational reasons, while vendors of security technology are incented to exaggerate the risk of attack[11]. Much of the research in this area is theoretical because information effects can be hard to isolate, measure and analyze in the real world. There are also few incentives for organizations to share information regarding their decision-making processes and shortcomings. Data protectionism by organizations results in inadequate access to information about specific cyber incidents and ultimately longitudinal cyber risk trends.

As well, the focus of current cyber-risk research is highly correlated with the availability of data or the ease with which data can be acquired. While this may be unsurprising, it reflects a ground truth that research focus and even findings may be disproportionately driven by data availability rather than the most interesting and significant capability gaps. For example, there is considerable research surrounding data breaches because of the relative availability of this type of data (quality variability notwithstanding), while there is very little on control performance.

Though the number and scope of data resources is increasing, as the U.S. 2016 Federal Cybersecurity R&D Plan points out, "…many are unable to deal with proliferation of massive data sets, do not support semantically rich data searches and have limited data provenance information[3]."

Examples of research objectives across this theme are:

- Provide policymakers, regulators and other decision-makers an empirically-based analysis of the impact of inadequate information on the cyber ecosystem
- Catalog data assets, needs and requirements for fusing cyber-logical, cyber physical, cross-domain, economic, behavioral, societal, and environmental data to address specific cyber security challenge problems
- Build and make available scalable and sustainable data assets for government, researcher and industrial use in cybersecurity evaluation and decision making
- Augment the DHS S&T IMPACT resource platform[4] with valuable data produced in the course of government-funded R&D that would otherwise go unused as well as with contributions from industry that would improve organizational and collective capacity to develop, test and evaluate cybersecurity knowledge and technology products and services
- Empirically model incentives and ROI for data sharing[5]

F. Threat Dynamics

The most obvious challenge to research on threat dynamics is the hidden nature of attacks and attackers. Attackers also have varying motivations (e.g., economic vs political) and resources (e.g., nation-state vs. individual hacker) to attack, adding to the challenge of modeling adversary behavior. Finally, the attack vectors change frequently, at least among the most sophisticated attackers. Law enforcement is often prevented from sharing data seized in a case due to legal restrictions. Researchers are challenged to remain on the right side of the law and ethics in their quest to facilitate understanding of cyber-criminal activity.

Examples of research objectives across this theme are:

- Understand how attackers decide on targets and methods for attack
- Develop protection, response and recovery strategies based on knowledge of attacker objectives
- Identify intervention points where threat operations are susceptible to disruption
- Understand how investment in controls can alter attacker behavior
- Develop analytic frameworks to characterize the evolution of cybercriminal enterprises
- Identify potential disincentives for cyber criminals
- Develop metrics for standardizing the evaluation of threat data

REFERENCES

[1] The White House, Executive Order – Improving Critical Infrastructure Cybersecurity, February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

---

[4] IMPACT portal: https://ImpactCyberTrust.org; Department of Homeland Security, Science and Technology Directorate, Cyber Security Division, Information Marketplace for Policy and Analysis of Cyber-risk & Trust, https://www.dhs.gov/csd-impact.

[5] The DHS S&T CYRIE program awarded a contract to the University of Tulsa under the direction of Dr. Tyler Moore to study data production and usage by cybersecurity researchers, information that will help quantify the value of data-sharing and improve sharing incentives to address the interdependency of cyber-risk environments, Grant Number FA8750-17-2-0148.

[2] The White House, Presidential Policy Directive – Critical Infrastructure Security and Resilience, February 12, 2103. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience.

[3] National Science and Technology Council, Networking and Information Technology Research and Development Program, Federal Cybersecurity Research and Development Strategic Plan, February 2016.

[4] Computing Research Association. "Four Grand Challenges in Trustworthy Computing." 2003.

[5] Liu, Yang, et al. "Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents," USENIX Security, August 2015, Washington, D.C.

[6] Sarabi, Armin, et al. "Risky business: Fine-grained data breach prediction using business profiles," Journal of Cybersecurity, 2(1), 2016, 15-28.

[7] Moore, Tyler, et al. "Identifying How Firms Manage Cybersecurity Investment." 15th Workshop on the Economics of Information Security. University of California Berkeley, Berkeley, California, USA. 13-14 June 2016.

[8] Friedman, Sam and Thomas, Adam. "Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market." https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html.

[9] E.g., Eling, Martin and Schnell, Werner. "What do we know about cyber risk and cyber risk insurance?", The Journal of Risk Finance, 2016, vol. 17, issue 5, pp. 474-491.

[10] Mersinas, Konstantinos, et al. "Experimental Elicitation of Risk Behaviour amongst Information Security Professionals," 14th Workshop on the Economics of Information Security. Delft University of Technology, the Netherland. 22-23 June 2015.

[11] Anderson, Ross. "Why Information Security is Hard—An Economic Perspective." Proceedings of the 17th Annual Computer Security Applications Conference (2006), 610-13.