



# Cyber Risk Economics Capability Gaps Research Strategy

2018



**Homeland  
Security**

Science and Technology



# EXECUTIVE SUMMARY

Cybersecurity is a multidimensional challenge that demands interdisciplinary attention. The Department of Homeland Security Science and Technology Directorate (DHS S&T) Cyber Risk Economics (CYRIE) program supports research, development, and operationalization of technical and knowledge solutions that improve value-based decision making by those who own, operate, protect, and regulate the nation's vital data assets and critical infrastructures. The focus extends beyond the traditional economics view of incentives for cybersecurity to consider business, legal, technical, and behavioral factors that impact cyber risk. CYRIE R&D emphasizes the empirically based measurement, modeling and evaluation of cybersecurity investment, impact and incentives.

This research strategy is directed at public and industrial researchers and funding organizations for the benefit of cybersecurity stakeholders across industry and government. It frames a series of research opportunities that address 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 most challenging issues in cybersecurity. The objective of this paper and the CYRIE program is 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.

The strategy describes 12 research areas organized into 6 themes, as follows:

 <b>THEME 1: THE QUANTIFICATION OF RISK</b>	Area 1 – Entity Risk Assessment Area 2 – Systemic Risk Assessment Area 3 – Impact of Controls Area 4 – Decision Support
 <b>THEME 2: ROLE OF GOVERNMENT, LAW, AND INSURANCE</b>	Area 5 – Role of Government Regulation Area 6 – Role of Insurance Area 7 – Role of Law and Liability
 <b>THEME 3: THIRD PARTY RISK</b>	Area 8 – Supply Chain Accountability
 <b>THEME 4: ORGANIZATIONAL BEHAVIOR AND INCENTIVES</b>	Area 9 – Organizational Effectiveness
 <b>THEME 5: DATA COLLECTION AND SHARING</b>	Area 10 – Information Asymmetries Area 11 – Data Collection and Mapping
 <b>THEME 6: THREAT DYNAMICS</b>	Area 12 – Adversary Behavior and Ecosystem

# EXECUTIVE SUMMARY

Each research area is framed in terms of current gaps in capability or understanding, known or expected challenges to the development of solutions, and key research objectives. The research opportunities below are representative of what follows in the strategy:

## **AREA 1 – ENTITY RISK ASSESSMENT**

Understand the key organizational attributes around which risk (nature, severity, probability) is distributed, such as third-party relationships, customer base size, type of information stewarded, and online footprint

## **AREA 2 – SYSTEMIC RISK ASSESSMENT**

Develop and validate metrics and measures of the degree, effect, and location of correlated and concentrated risk

## **AREA 3 – IMPACT OF CONTROLS ON RISK**

Collect, inventory, and analyze empirical data that maps experience with specific cybersecurity controls to outcomes

## **AREA 4 – DECISION SUPPORT**

Evaluate framework effectiveness in supporting decision making, including any systematic gaps or biases in controls investment that may result from their use

## **AREA 5 – ROLE OF GOVERNMENT REGULATION**

Develop comparative analyses and recommendations for proper application of incentives instruments such as preferred procurement, tax, subsidies, liability, or regulation

## **AREA 6 – ROLE OF INSURANCE**

Develop mechanisms for broader and more effective use of relevant environmental data in cyber insurance underwriting

## **AREA 7 – ROLE OF LAW AND LIABILITY**

Study how existing product liability frameworks may be applied to address cybersecurity failures in the context of increasingly connected networks and devices, for example in the automotive, medical, and building controls sectors

## **AREA 8 – SUPPLY CHAIN ACCOUNTABILITY**

Understand and quantify how coordination costs factor into shared security contexts

## **AREA 9 – ORGANIZATIONAL EFFECTIVENESS**

Assess the relative value of security and risk culture in an organization versus security controls

## **AREA 10 – INFORMATION ASYMMETRIES**

Examine how information deficits affect cybersecurity risk management

## **AREA 11 – DATA COLLECTION AND MAPPING**

Catalog data assets, needs and requirements for fusing cyber-logical, cyber physical, cross-domain, economic, behavioral, societal, and environmental data to address specific cybersecurity challenge problems

## **AREA 12 – ADVERSARY BEHAVIOR AND ECOSYSTEM**

Develop metrics for standardizing the evaluation of threat and attack data

There is naturally some overlapping of gaps and research challenges across the construction of themes. Irrespective of the overlap, progress toward solutions to these problems is intended to improve real world cyber risk management.

# TABLE OF CONTENTS

i	<b>Executive Summary</b>
2	<b>Introduction &amp; Background</b>
2	Purpose
3	Approach
5	Research Themes and Areas
6	<b>Theme 1: The Quantification of Risk</b>
7	<b>Area 1 – Entity Risk Assessment:</b> Measuring the nature, size, frequency, and consequences of cyber risks at the entity level
9	<b>Area 2 – Systemic Risk Assessment:</b> Measuring the nature, size, and frequency of cyber risks in the ecosystem, including correlated and interdependent risk
11	<b>Area 3 – Impact of Controls:</b> Evaluating how investment in controls changes risk and outcomes
13	<b>Area 4 – Decision Support:</b> Understanding and improving control investment decision making
15	<b>Theme 2: Role of Government, Law, and Insurance</b>
16	<b>Area 5 – Role of Government Regulation:</b> Assessing the impact of cybersecurity regulation on cyber risk and outcomes
17	<b>Area 6 – Role of Insurance:</b> Understanding the effects of insurance on cybersecurity investment and cyber risk and outcomes
20	<b>Area 7 – Role of Law and Liability:</b> Understanding the effects of law and liability on cyber risk and outcomes
23	<b>Theme 3: Third Party Risk</b>
24	<b>Area 8 – Supply Chain Accountability:</b> Approaches for improving accountability for security within complex supply chains
26	<b>Theme 4: Organizational Behavior and Incentives</b>
27	<b>Area 9 – Organizational Effectiveness:</b> Evaluation of the organizational characteristics associated with effective cybersecurity
28	<b>Theme 5: Data Collection and Sharing</b>
29	<b>Area 10 – Information Asymmetries:</b> Identify how information deficiencies and asymmetries in the ecosystem affect risk, behavior, decisions, and outcomes
30	<b>Area 11 – Data Collection and Mapping:</b> Development of tools for efficient and systematic collection of cyber environmental data, and correlation/translation to business-centric data and metric
32	<b>Theme 6: Threat Dynamic</b>
33	<b>Area 12 – Adversary Behavior and Ecosystem:</b> Understanding the behavior and decision making of attacker
34	<b>Conclusion</b>
35	<b>References</b>

# INTRODUCTION & BACKGROUND

Cybersecurity is a multidimensional challenge that demands interdisciplinary attention. The Department of Homeland Security Science and Technology Directorate (DHS S&T) Cyber Risk Economics (CYRIE) program [1] supports coordination and research into the business, legal, technical, and behavioral aspects of cyber risk<sup>1</sup> economics relative to cyber threats, vulnerabilities, attacks, and controls.<sup>2</sup>

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.<sup>3</sup> These policy documents gave DHS a coordinating role in pursuing the cybersecurity objectives outlined in each document and directed 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 cyber economic incentives, through its R&D efforts and portfolio. Another executive order issued in May 2017 directs DHS and the Department of Commerce to report on sufficiency of existing Federal policies and practices to promote market transparency for cybersecurity risk management by critical infrastructure entities.<sup>4</sup>

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

In May 2018, DHS issued a cybersecurity strategy that provides a framework to keep pace with the evolving cyber risk landscape by identifying digital risks, reducing threats and vulnerabilities, mitigating cyberattacks, and; and making the cyber ecosystem more secure and resilient.<sup>5</sup> This Cyber Risk Economics Research Strategy and the S&T CYRIE program's research priorities support and align with the DHS Cybersecurity Strategy.

## Purpose

The S&T 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 infrastructures. 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, technical, and behavioral factors. In this way CYRIE R&D can more effectively address strategy and tactics for cyber risk avoidance, acceptance, mitigation, and transfer.

<sup>1</sup> The DHS Risk Lexicon [2] defines Risk as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. We have adopted the following additional definitions for this Strategy document: a Threat is a specific source or method of cyberattack; an Attack is an attempt to exploit a vulnerability (actual or perceived) in an effort to do harm; a Vulnerability is a weakness, flaw, or gap in the security of a given asset that allows an attack to be successful.

<sup>2</sup> The technical and administrative measures put in place to minimize cyber security risk.

<sup>3</sup> Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity [3], and Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience [4].

<sup>4</sup> Executive Order 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [5].

<sup>5</sup> DHS Cybersecurity Strategy [6].

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;
- **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.<sup>6</sup>



Recognizing the importance of data sharing to building capacity across these four dimensions, the CYRIE program 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 threats evolve more quickly, and attacks spread more widely than defensive controls are capable of addressing. More collective information is needed to enable value-based risk management of the shared ecosystem. Effective information sharing can help mitigate against the often-siloed view of risk, create positive network effects, and foster “RoS” or return on sharing as an element of cyber risk management.

The CYRIE program 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.

## Approach

This research strategy frames a series of research areas that address capability gaps drawn from a confluence of authoritative documents highlighted in the Introduction, scholarly literature review, and a range of recent stakeholder discussions of cyber risk economics. These gaps comprise many of the most challenging issues in cybersecurity economics. Progress toward solutions to these problems is intended to improve real world cyber risk management. One goal of the strategy is to motivate and guide the work of academic and industry researchers. In parallel, this strategy is aimed at helping government and other funding sources identify and prioritize areas of investment. The expected output from research in these areas contemplates the creation of new data, measurements, models, and metrics. The objective of this strategy and the CYRIE program is 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.

<sup>6</sup> Risk Management is used herein to describe the “process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken” as defined in the *DHS Risk Lexicon* [2].



# INTRODUCTION & BACKGROUND

Three broad categories of input were used to guide the formulation of the research areas:

1. Insights and ground truth gleaned from several 2017 Stakeholder Exchange Meetings (SEMs) on Cyber Risk Economics research, stewarded by the Cyber Security Division within 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 cybersecurity economic identified the state of the art of CYRIE-related 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 2016 Federal Cybersecurity R&D Strategic Plan [7].

This Cyber Risk Economics Research Strategy and the S&T CYRIE program's research priorities are intended to support and align with the 2018 DHS Cybersecurity Strategy and associated Implementation Plan [8], as well as the recently created National Risk Management Center (NRMC) which aims to provide national coordination for collaborative, sector-specific and cross-sector risk management efforts to better protect critical infrastructure [9].



## Research Themes and Areas

This CYRIE research strategy describes the following 12 research areas organized into six themes:

 <p>THEME 1: <b>THE QUANTIFICATION OF RISK</b></p>	<p>Area 1 – Entity Risk Assessment Area 2 – Systemic Risk Assessment Area 3 – Impact of Controls Area 4 – Decision Support</p>
 <p>THEME 2: <b>ROLE OF GOVERNMENT, LAW, AND INSURANCE</b></p>	<p>Area 5 – Role of Government Regulation Area 6 – Role of Insurance Area 7 – Role of Law and Liability</p>
 <p>THEME 3: <b>THIRD PARTY RISK</b></p>	<p>Area 8 – Supply Chain Accountability</p>
 <p>THEME 4: <b>ORGANIZATIONAL BEHAVIOR AND INCENTIVES</b></p>	<p>Area 9 – Organizational Effectiveness</p>
 <p>THEME 5: <b>DATA COLLECTION AND SHARING</b></p>	<p>Area 10 – Information Asymmetries Area 11 – Data Collection and Mapping</p>
 <p>THEME 6: <b>THREAT DYNAMICS</b></p>	<p>Area 12 – Adversary Behavior and Ecosystem</p>

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

- Current gaps in capability or understanding
- Known or expected challenges to the development of solutions
- Key research objectives

## THEME 1

# THE QUANTIFICATION OF RISK



## THEME 1:

# THE QUANTIFICATION OF RISK



### AREA 1 – ENTITY RISK ASSESSMENT

Measuring the nature, size, frequency, and consequences of cyber risks at the entity level

#### Current Gaps

A lack of understanding and effective assessment of cyber risks among organizational leaders remains a fundamental challenge in cybersecurity. As early as 2003, the Computing Research Association [10], 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 risk models. This challenge was reaffirmed in the 2011 Strategic Plan for the Federal Cybersecurity R&D Program:

“There is no scientific basis for cost risk analysis, and business decisions are often based on anecdotes or un-quantified arguments of goodness.” [11] The 2016 Federal Cybersecurity R&D Strategic Plan reiterates the need to support “research in economic ecosystem externalities to enable understanding of the impact of trust and organizational design on cybersecurity decisions, as well as the role of micro- and macroeconomics in the design, construction, and operation of software, hardware, and systems.” [7] The 2018 DHS Cybersecurity Strategy emphasizes the need for DHS to work with government and other Homeland Security Enterprise (HSE) stakeholders to gain an adequate understanding of the national cybersecurity risk posture, analyze evolving interdependencies and systemic risk, and assess changing techniques of malicious actors.

**Organizational leaders’ lack of understanding and effective assessment cyber risks remains a fundamental challenge in cybersecurity.**

Absent such useful quantitative methods, organizational leaders tend to:

- Rely exclusively on qualitative measures of risk when making investment decisions
- Use breaches as a proxy measure of risk, including the occurrence of breaches (as high risk) and lack of breaches (as low risk)
- Focus disproportionality on vulnerabilities relative to threats
- View threats, vulnerabilities, and controls as static, rather than evolving over time and increasing in sophistication
- Ignore consequences of cyber incidents for external entities such as suppliers, customers, and the public

Even where organizations have developed risk assessments that consider cybersecurity factors, many are incomplete (e.g., they don’t include all relevant dependencies) and/or they are incompatible with approaches used by other organizations. Organizations developing standalone approaches to cybersecurity is problematic because cyber risk cannot be bounded and controlled in isolation from linkages and system dependencies to other entities.

#### Solution Challenges

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. Many business executives are confident their security levels are sufficient [12], and many know that their organizations will not



## THEME 1:

# THE QUANTIFICATION OF RISK

bear the full cost of successful attacks. 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 publicly accessible network data show promise that quantification challenges can be overcome [13][14]. Risk rating firms offer cybersecurity scoring of organizations for self-comparison or third-party vendor management.<sup>7</sup> Notably, however, a key challenge to more accurate and complete risk understanding is accumulating risk measures from inside companies and correlating these with externally-observable risk data and with actual loss event data.



### Research Objectives

- Recognize and forecast the key spatial, temporal and relational attributes around which organizational risk (nature, severity, probability) is distributed, e.g., third-party relationships, customer base size, type of information stewarded, and online footprint
- Develop techniques to distinguish lagging from leading indicators of cyber risk
- Develop and improve organization-level resilience metrics, standard methods of assessment, and baselines that incorporate resilient designs and materials, response and recovery plans, resilient business processes, and human factors
- Create models to map cyber risk metrics to operational, financial, environmental, political, regulatory, and technology risk
- Evaluate the nature of: the different asset categories value, the cyber risk to a range of categorical assets, and the magnitude of potential harm that may accrue to each asset category (i.e., tangible physical assets, and intangible assets such as data, intellectual property, software, goodwill and reputation, R&D, and business process)
- Evaluate how the magnitude of risk varies by source of risk, e.g., external attackers, malicious insiders, negligent practices, systems and technical failures, internal process failures, etc.
- Evaluate the comparative implications for risk management of focusing on different units of analysis, e.g., asset-level risk versus organization- or sector-level risk
- Develop tools and mechanisms to communicate cyber risk to executive and other non-technical audiences for decision support
- Identify the circumstances under which different types of organizations face existential risk from cyber threats (i.e., go out of business)
- Develop organizational-level cyber risk management models that are both prescriptive and flexible to evolve with changing risk composition
- Identify and characterize dependency and interdependency dynamics for entity risk assessment methodologies

<sup>7</sup> Examples include companies such as Bitsight, FICO, Cyence, and SecurityScorecard.



## AREA 2 – SYSTEMIC RISK ASSESSMENT

Measuring the nature, size, and frequency of cyber risks in the ecosystem, including correlated and interdependent risk

### Current Gaps

We lack integrated and scalable adoption and application of systemic risk assessment, resulting in ineffective and uncoordinated application of resources for cybersecurity.<sup>8</sup> There is insufficient knowledge about the risks facing critical infrastructure networks<sup>9</sup> as well as the frequency and impact of cyberattacks on the cumulative components systems and associated data [17][18]. The same is true for risk and impact across organizations and sectors that share common cyber resources. Resulting effects on the economy; safety, security, and social order; and, confidence in public and private institutions are widely inconsistent and variable at best, and nonexistent at worst. Current assessment approaches have limited ability to reliably consider low probability, high-consequence cyber events. We know from practice that cyber risk is not independent and is highly correlated across organizations in an ecosystem. Game theory and other more theoretical assessments highlight numerous mechanisms by which this interconnected risk arises and plays out [19][20][21][22][23][24]. The 2015 National Critical Infrastructure Security and Resilience R&D Plan and the 2018 DHS Cybersecurity Strategy call out the development of risk assessment and management approaches that consider ecosystem-wide effects as a research priority [25].

There is insufficient knowledge about the risks facing critical infrastructure networks, as well as the frequency and impact of cyberattacks on the cumulative components systems and associated data.

In addition to a limited understanding of the correlation of risk across the ecosystem, we have an imperfect view of where risk is concentrated. For example, at the ecosystem level, there is currently no effective way to assess in what sectors or firm sizes risk is concentrated. This makes it difficult to know where changes in controls could have the greatest impact in ecosystem-wide risk reduction. Risk can be assessed at the asset level (e.g., via software quality assurance, malware analysis, vulnerability testing, intrusion detection), and to some degree at the organization level. Yet, there is little understanding of how to roll this up to assess the cybersecurity risk exposure at larger scales, up through a macroscopic level. Estimates of risk or harm all too often mistakenly induce systemic risk by amassing specific risks or use attributes that do not map to real risk (e.g., using a company's market share rather than company-specific risk attributes to assess aggregate risk). As well, the lack of common lexicon and associated semantics to communicate systemic risk is both a symptom of and contributor to our collective lack of command of systemic risk.<sup>10</sup>

<sup>8</sup> Noting that guidelines do exist, for example, NIST 800-30 Guide for Conducting Risk Assessments [15]. As discussed in Theme 5, systemic risk assessment is beset by underlying quantitative measurement difficulties which contribute to process adoption and application challenges.

<sup>9</sup> PPD-21 [4] identifies 16 critical infrastructure sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems. In January 2017, DHS designated election Infrastructure as a critical infrastructure subsector under the government facilities sector [16].

<sup>10</sup> The Zurich Global Risks Report 2016 [17] corroborates this notion, "Two workshops were held to assess the nature of systemic cyber risk, and dozens of interviews and discussions were conducted with recognized global experts, owners, operators and senior private- and public-sector leaders. One finding was consistent – the meaning and implications of systemic cyber risk are not yet fully recognized or understood."



## THEME 1:

# THE QUANTIFICATION OF RISK



### Solution Challenges

It can be quite challenging to coordinate and incentivize frameworks to support complementary risk management and assessment approaches among a variety of stakeholders, whether that be at the organizational, community, sector, national, international, or other level of shared interest. Much current knowledge of risk is derived from estimates of breach frequency and impact from surveys or analyses of aggregated data that is mandated to be disclosed. These sources of data concern perceived or surmised activity related to assets at the firm level, not forensic details related to interconnected systems or networks from which aggregated risk stems. As well, these data reflect only a fraction of the breach landscape and cannot be rationally compared because syntax and semantics related to technical and financial details diverge from one source to another. Further, these studies vary widely on estimates of the size, frequency, and severity of attacks, suggesting fundamental data inadequacy across the board. For example, widely-cited industry reports and those mentioned in the media consistently point to the high cost of breaches. In 2017 one oft-quoted survey organization [26], for example, reports an average breach cost of \$3.62M, while academic studies indicate that neither the size nor frequency of data breaches have increased over the past decade [27], and that the mean breach cost is only \$200K, or 0.4% percent of total firm revenue [28].

There is a range of challenges to addressing these gaps, including:

- Reluctance by organizational leadership to incorporate more complete (i.e., external cyber dependencies) and standardized risk assessments and/or share relevant data that is prerequisite to accurate understanding of externalities, dependencies across systems, and downstream effects
- Survey and other self-reported data that are often self-serving and otherwise biased/unrepresentative
- Higher risks may be faced by smaller organizations, where behavior and controls investment are harder to measure
- The low-odds/high-consequence nature of the most impactful systemic risk, which exacerbates measurement and modeling difficulty
- Skewed target valuation (e.g., [29])
- Diversity and dynamic attacker motivations and incentives



### Research Objectives

- Develop and validate metrics and measures of the degree, effect, and location of correlated and concentrated risk within the ecosystem
- Measure and model risk pooling as a risk transfer and mitigation strategy
- Identify and evaluate cyber dependencies and cascading impacts at macroscopic levels, i.e. in aggregate across an ecosystem
- Assess the share of ecosystem risk accounted for by specific groups of organizations with low-hanging opportunities for risk mitigation
- Build models to relate asset-level risk to organizational-level risk and ecosystem-level risk
- Collect historical data and develop analytic models to predict ecosystem conditions after the occurrence of a high-consequence/low-probability event
- Develop models that improve the ability to describe complex systems with more precision in order to enhance the quality and fidelity of risk assessments for decision makers





- Develop evaluation methods and processes for resilience capabilities, and quantify uncertainty for those evaluations
- Develop analytics that identify and characterize security properties of connections between networks and systems, e.g., identify and characterize relationships between security properties at different layers along the OSI stack, network mapping and inter-domain internet topology
- Develop integrated risk assessment and profile methodologies across critical infrastructures, sectors, and organizations that consider a range of consequences and externalities associated with disruptions to primary assets or systems of interest. This would involve:
  - Integrating best practices and functional requirements for identifying critical assets and business processes and their associated risks
  - Considering factors such as resilient designs and materials, response and recovery plans, resilient business processes, and human factors
  - Linking the shared functions across the systems in question to the critical infrastructure that provides enabling services
- Develop models and data schema that address:
  - Probability of attacks on particular critical infrastructures
  - Locations of risk accumulation/aggregation
  - Impacts of cascading effects across critical infrastructure sectors
  - Magnitude and value of losses from the cyber-related theft of intellectual property
  - Magnitude and value of losses stemming from reputational harm to companies following cyber incidents, such as data breaches and service failures (e.g., business interruption)

### AREA 3 – IMPACT OF CONTROLS ON RISK

Evaluating how investment in controls changes risk and outcomes

#### Current Gaps

Organizations have a deficient understanding of how investment in controls changes their risk levels, making it difficult to choose the appropriate level of investment. Even when security standards can be established, they have not been predictably mapped to measures of effectiveness of controls. Disagreement on metrics and measurement of harm, essential to defining the severity of impact, further compounds the challenge. Harm in the broad sense can include direct and indirect economic loss; loss or compromise of data; reputation damage; lost time and productivity; privacy liability; damage to business processes; cost of remediation and protective measures; loss of trust and social destabilization; interruption of civil commercial, government, and defense activity; and damage to physical systems and critical infrastructure. Thus, organizations are challenged to prioritize spending on and placement of controls across areas of risk. Upgrading systems with newer technologies can serve as a control against security risk posed by legacy technologies, however, upgrade costs are inevitably met with resistance.

Organizations have a deficient understanding of how investment in controls changes their risk levels, making it difficult to choose the appropriate level of investment.





## THEME 1:

# THE QUANTIFICATION OF RISK

The 2018 DHS Cybersecurity Strategy further identifies the need for the Department to improve the development and deployment of tools, services, and other offerings to stakeholders, as well as the DHS's understanding of the efficacy and utilization of such tools and services. It also recognizes the importance of engaging with officials at the appropriate levels within an organization to ensure that gaps in critical infrastructure cybersecurity involving potentially significant impacts on national security, public health and safety, or economic security are addressed.



### Solution Challenges

The correlation between risk and control implementation is difficult to analyze because the relationship is complex and mediated by numerous hard-to-measure endogenous and exogenous variables. Data tends to be scarce, as neither breached organizations nor vendors are inclined to disclose details regarding cybersecurity breaches. Security audits are often inadequate for estimating future impact of control implementation, since cyber threats can evolve quickly, rendering one-time analyses obsolete. As well, it can be difficult to evaluate the effectiveness of individual controls or select the right set of controls in the presence of multiple vendors. Finally, as behavioral economics foretells, it is common for organizational leaders to invest in controls reactively (after a cyberattack with damaging consequences), rather than proactively.



### Research Objectives

- Quantify how investments in specific controls change risk and outcomes
- Collect, inventory, and analyze empirical data that maps experience with specific cybersecurity controls to outcomes
- Develop value- and outcome-based metrics and measurements for assessing efficacy of technical controls.
- Comparative analysis of how we model cybersecurity controls effectiveness versus how we actually use those controls
- Understand the comparative impact of hard controls versus that of soft controls<sup>11</sup>, and assess the relationship they have on the effectiveness of each other
- Understand and quantify harm from a socio-technical perspective, rather than from the perspective of how harm is enshrined in current law
- Estimate the risk remaining if there were universal adherence to baseline, minimal cybersecurity standards, e.g., such as described by Nationwide Cyber Security Review (NCSR)<sup>12</sup>
- Develop models, simulations, and exercises that communicate the full range (direct to indirect) of the impacts of cyber incidents using information that incorporates both technical details and human decision making

<sup>11</sup> "Hard controls" refer to physical and technical controls, whereas "soft controls" refer to administrative-related measures such as governance, regulation, law, policy, training, and best practice.

<sup>12</sup> The Nationwide Cyber Security Review (NCSR) is a free, anonymous, annual self-assessment survey that is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and is sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).



## AREA 4 – DECISION SUPPORT

### Understanding and improving control investment decision making

#### Current Gaps

While organizational decision support for business risk<sup>13</sup> is universally proven and accepted, organizations find traditional investment decision tools to be of limited use for cybersecurity risk management. Most organizations rely instead on frameworks [30], 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. Industry attention and action focuses on improving processes (reinforced by frameworks) which can lead to check-box compliance, rather than focusing on outcomes. Decision support frameworks predominate cybersecurity risk management and a variety of approaches are available to assess risk, some of which are widely used.<sup>14</sup> Yet there is currently little empirical evidence of the effectiveness of decision support frameworks on investment in controls and ultimately reduction in risk.

While organizational decision support for business risk is proven and accepted, organizations find traditional investment decision tools to be of limited use for cybersecurity risk management.

As well, cyber risk is often treated as an information technology (IT) problem rather than as a component of organizational risk management strategy. Cyber risk metrics 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 [30]. As a result, cyber risks are less likely to receive necessary attention and resources.

#### Solution Challenges

Framework use has been studied in some detail in [30], but effectiveness is hard to measure, as inappropriate or ineffective framework application are often confounding factors. Even when frameworks are applied as intended, organizations have different vulnerabilities and threat profiles. As well, it is premature to assess the effectiveness of some contemporary, standard frameworks (e.g., NIST CSF) since widespread adoption is relatively recent.

#### Research Objectives

- Evaluate framework effectiveness in supporting decision making, including any systematic gaps or biases in controls investment that may result from their use
- Develop models that help translate framework output into concrete measurements of risk
- Explore how frameworks can be used by governments to encourage investment in cybersecurity controls
- Develop hybrid approaches that integrate both process- and data-driven framework models for cybersecurity decision making

<sup>13</sup> For example, investment, liquidity, assets and liabilities, market, credit and underwriting/retention risks.

<sup>14</sup> See, for example, FAIR [31], the Cyber Defense Matrix [32], and the Cyber Prep approach of MITRE [33].



## THEME 1:

# THE QUANTIFICATION OF RISK

- Understand how limits to organizational resources affect decision making with respect to cybersecurity investment
- Design mechanisms to bridge communication (semantic and syntactic) gaps between organizational leadership and security staff, e.g., translate and align cyber risk to familiar financial risk terms; develop gap analytics for financial exposure based on cyber risk frameworks; and quantify variables used in common value calculations such as Return on Security Investment, Annual Rate of Occurrence, Annual Loss Exposure, and Single Loss Exposure
- Develop value- and outcome-based measures and metrics for framework-based risk management

## THEME 2

# ROLE OF GOVERNMENT, LAW, AND INSURANCE





## THEME 2:

# ROLE OF GOVERNMENT, LAW, AND INSURANCE

### AREA 5 – ROLE OF GOVERNMENT REGULATION

Assessing the impact of cybersecurity regulation on cyber risk and outcomes

#### Current Gaps

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 direct and indirect compliance costs. Economic models of the effects of regulation on cybersecurity are largely theoretical and variable with respect to predicted effectiveness [30][34][35][36]. Most policy tends to focus on consumer protection, and less emphasis is placed on critical infrastructure protection. Empirical research on regulatory impacts tend to focus on breach notification laws and immediate economic losses such as subsequent identity theft. This research generally shows notification laws to be associated with a small reduction in breaches [37] and not necessarily desired changes in behavior, such as greater security investment and greater data protection.

**The impact of regulation on risk and outcomes in cybersecurity is critically important but evaluation to date has been limited.**

In addition to gaps in evaluating the role of regulation in cybersecurity, there are limitations with regulation itself, at least so far as industry perceives it. These limitations include:

- Absence of models to help regulators balance tensions between accountability and transparency, e.g., mandating detailed cybersecurity incident reporting, while also considering legitimate data sensitivity concerns
- Challenges to crafting regulation that is specific enough to avoid overreach yet broad enough to be constructive and future proof
- Relative static nature of regulation in the face of rapidly evolving threats, technology, information value, and criticality of systems
- Complexity generated by what is perceived as patchwork regulation that makes it difficult for organizations to respond strategically; some regulations encourage rule-based compliance rather than a risk-based, comprehensive strategic approach to cybersecurity



#### Solution Challenges

The impact of cybersecurity regulation is difficult to distinguish from myriad other effects, including those that manifest from the component level (e.g., the effectiveness of controls) to the ecosystem level (e.g., actions of attackers). In addition, the unintended consequences of regulation are difficult to model ex-ante. Finally, the cumbersome process by which policy is made, and the collective agreement needed to create it, makes regulation both hard to influence and hard to forecast.



## Research Objectives

- Understand the technical and behavioral variables that influence the effectiveness of cybersecurity regulation, as well as the specific attributes of cybersecurity-related regulations that impact the level of cybersecurity controls adoption
- Understand the circumstances under which regulation potentially degrades overall security practice and exacerbates systemic risk
- Develop models for “agile” cybersecurity compliance that can more effectively address emergent and dynamic threats rather than merely checking off boxes
- Identify the conditions, including a cost-benefit analysis, when government should act as coordinator and facilitator of industry-driven processes and those under which it should act as a top-down regulator of requirements
- Develop comparative analyses and recommendations for proper application of incentives instruments such as preferred procurement, tax, subsidies, liability, or regulation
- Develop mechanisms to help organizational leaders and end users understand and make more informed choices about cyber risks
- Develop the cyber equivalent of the financial Institution stress test<sup>15</sup>, the policy rationale for such a test, and the implementation framework by which it would operate
- Develop mechanisms to help government leaders and policy makers identify and analyze the likely secondary effects from government intervention, such as technological innovation, economic progress, and the rights and interests of individuals in society; this should include a mapping of likely consequences within a continuum of intervention types ranging from light touch activities to more interventionist measures
- Identify ways in which information disclosure and transparency requirements can be extended beyond data breach to other cybersecurity outcomes (e.g., categorical fraud loss, attacks on critical infrastructures, etc.); and develop approaches to minimize the adverse consequences of public disclosure while still providing actionable information (e.g., disclosure to public authorities of aggregated figures not attributable to affected organizations)

## AREA 6 – ROLE OF INSURANCE

Understanding the effects of insurance on cybersecurity investment and cyber risk and outcomes



### Current Gaps

Cyber insurance is not new by internet time horizons, although it is nascent relative to its health, automobile, and life counterparts. As such, many organizations do not yet know how to evaluate the benefits of insuring against cyber risk. The impact of cyber insurance on cyber risk for an individual organization and for an ecosystem are not well understood, and the benefits of cyber insurance to organizations connected to breached organizations is even less well understood.

<sup>15</sup> A financial stress test is an analysis designed to determine how resilient a given financial instrument or financial institution is to economic crisis.





## THEME 2:

# ROLE OF GOVERNMENT, LAW, AND INSURANCE

Perhaps the biggest challenge 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 [38]. On the underwriting side, lack of cybersecurity domain expertise and relevant actuarial information leads to policies that can be ill-fitting or otherwise over/under inclusive. Current practice relies on insurance rate multipliers for firmographics and cybersecurity hygiene applied to base pricing [39], though other approaches have been proposed (e.g., [40]) that attempt to accommodate the lack of data on actual losses. Rational and more risk-informed insurance underwriting require pragmatic quantitative risk assessment models, but the analytical tools and data available to insurance providers to translate controls investment and other measurable aspects of cybersecurity preparedness into price are immature. This lack of sophisticated underwriting means that organizations investing in stronger cyber controls are not guaranteed price concessions as a result of their efforts to reduce risk.

Perhaps the biggest challenge facing insurance markets is accurate risk quantification, which necessitates better data on cyber threats, vulnerabilities, attacks, and controls.

In addition to risk transfer, insurance might also be leveraged to incentivize risk reduction. While the industry has not traditionally embraced a role of standards promoter, the current chicken-and-egg dynamic with respect to cybersecurity standards, risk underwriting, and legal ordering forces has left a forcing function gap that is ripe to be filled. Theoretical economic research has shown that under certain modeling conditions, cyber insurance does not improve security (e.g., [41]), but these conclusions are based on traditional insurance business models. Without more empirical valuation of the relationship, and applied or even simulated innovative business models, it is hard to make effective policy decisions.

While automobile and health insurance domains are embracing targeted, near real-time behavioral and machine telematics, the cyber insurance industry has yet to engage “precision cyber insurance” in its underwriting, risk control, or claims processes. Ironically, though instrumentation and platforms for such measurements have existed since the advent of cyber insurance (e.g., intrusion detection systems, intrusion protection systems, risk measurement devices based on Security and Information Event Management or SIEM), they have yet to be integrated with insurance providers’ business policies and processes.

The insurance industry does not have a good grasp of costs of catastrophic event loss and therefore it lacks the ability to distinguish consequences that are insurable from those that are not. Insurers are starting to generate better loss figures around cyberattacks on specific industries but cannot yet effectively quantify the cascading effects on other sectors [42]. Identifying specific risk accumulators within organizations and certain industries has shown promise, but difficulties still remain in pricing the aggregated risk.

Furthermore, there is a dearth of scalable, sustainable cyber risk data-sharing regimes that support the needs of cyber insurers [43]. New disclosure control technologies that provably protect sensitive data need to be transitioned from the lab to the marketplace to overcome aversions to sharing data on breaches, controls effectiveness, and loss events [18], while preserving more beneficial sharing of data and collective information about Finally, organizational leaders with cybersecurity expertise (i.e., CISOs) should be included in cyber insurance decisions.





## Solution Challenges

The challenges to developing effective markets for cybersecurity insurance are well documented (e.g., [44]). Correlated and interdependent risks make analysis difficult, as does the presence of downstream harms to those other than insured parties. The same challenges that impede the emergence of efficient markets for cyber insurance (e.g., lack of data sharing about attacks, vulnerabilities, controls and impacts) also affect research into insurance markets. In addition, it is challenging to evaluate the specific tradeoffs organizations make between insurance and controls, as it requires a broad mix of data-gathering and research approaches. Other challenges include:

- Understanding if and to what extent moral hazard, adverse selection, and information asymmetry – all typical of insurance writ large – pose greater challenges in cyber insurance than in traditional insurance domains (home, auto, health, property) because of the dynamic threats and interrelated security environment
- Addressing the risk dependencies (i.e., shared platforms, software, connectivity) that make loss attribution and liability assignment difficult
- Requiring specific technical controls as a condition for coverage is challenging for carriers because it can be difficult for them to audit/verify client use of such controls



## Research Objectives

- Quantify the ecosystems-wide effect of insurance on risk exposure and resiliency
- Understand the strategies, institutional requirements and conditions under which multi-party insurance can enable coverage for aggregated and correlated risk (i.e., “risk pooling”)
- Develop models for identifying risk diversity in a dynamic threat environment and for adjusting mitigation strategies based on levels of dynamism
- Develop proof-of-concepts and prototypes and conduct pilots of socio-technical mechanisms that incentivize the sharing of valuable insurance data in a manner that addresses competitive the advantage concerns of issuers
- 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 assets and architecture data, security technologies and platforms in use, scope and nature of sensitive data, critical control systems in use)
- Develop and prototype innovative policy instruments; for example, agile policies that are temporally and spatially responsive to the specific risk attributes of the ‘measured organization’; policies tailored to incentivize investment in controls, but which limit insurer’s exposure by pooling risk
- Develop models, simulations, and exercises to continually improve understanding of risk accumulation and more accurately estimate probable maximum loss arising from a particular cyber incident– up to and including catastrophic loss
- 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
- Comparatively analyze and model the effect of current and potential government backstopping of cyber insurance on industry growth (e.g., the Terrorism Risk Insurance Act of 2002 (TRIA) [46] and the DHS SAFETY Act post 9/11 [47])



## THEME 2:

# ROLE OF GOVERNMENT, LAW, AND INSURANCE

## AREA 7 – ROLE OF LAW AND LIABILITY

Understanding the effects of law and liability on cyber risk and outcomes

### Current Gaps

The law is a fundamental mechanism to influence, and control the behavior of a democratic society and is a reflection of the collective expectations. Laws are created via Congressional legislation, Executive branch Orders, or judicially-created precedent. Risk is an unavoidable and expected byproduct of society's use of technology. Liability – whether imposed by public or private (contract) law – can limit the adverse impacts of technology by incentivizing prudent behavior and control of technology-related risk in order to avoid, minimize or mitigate harm, loss and damage. Certain trends have developed in the interpretation and application of law that have diminished the role of liability as a forcing function on organizational behavior toward cyber risk. For example, courts addressing cases that seek legal recourse for cybersecurity and data breach events have largely dismissed them for failure to establish standing or prove cognizable damage and actionable harm.<sup>16</sup>

The uncertainty surrounding standards for cybersecurity further illustrates where the behavioral forcing function of liability is weakened. The ability to hold an organization responsible for failure to meet its duty to protect data under a negligence claim, state cybersecurity law, or federal unfair and deceptive trade practices regulation often depends upon whether a standard has been met. While some progress has been made at the state level<sup>17</sup>, in lieu of clearer guidance as to what are acceptable security practices beyond vague 'reasonable and appropriate' language, case law will remain inconsistent at best and bereft of widescale risk shaping forcefulness at worst. As well, arguably successful models<sup>18</sup> where liability has incentivized risk-sensitive behavior in connected risk environments have not been extended proportionately to the level of the cyber risk. Outside of the regulated healthcare sector, transitive risk sharing or transfer by way of contractual or regulatory requirements to purchase cyber insurance or otherwise warrant data security as a cost of doing business have yet to gain widespread footing.

**Risk sharing by way of contractual or regulatory requirements to purchase cyber insurance has not gained widespread footing.**

Despite the current conditions, there are mounting public concerns and social pressure to address breaches that impact sensitive data threaten to alter liability jurisprudence (e.g., [46]). Organizations are largely ill-prepared to address this potentially shifting tide. Nevertheless, certain policy and legal frameworks offer promising models to incentivize risk mitigation.<sup>19</sup> The financial services Payment Card Industry (PCI) standard, for example, poses a strong organizational behavior forcing function by de-certifying members whose online merchant fraud

<sup>16</sup> At this writing, there is a split in the U.S. Circuit Courts. While some do not recognize risk of future harm as conferring standing, others recognize an allegation of future harm if, for example, there is "danger of sustaining some direct injury" that is "both real and immediate"—such as identity theft.

<sup>17</sup> For example, California Technology Letter 18-01 [44] and New York NYDFS Cybersecurity Regulation 23 NYCRR Part 500 [49] have deemed minimum standards whereby each Covered Entity's cybersecurity program must perform six "core" functions.

<sup>18</sup> For example, the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act are laws that have instituted a transitive risk regime whereby business associates of a covered organization must implement and attest to proper data privacy and security controls or face steep penalties.

<sup>19</sup> Under current liability conditions, organizations may be undertaking very good risk "management"—they rationally weigh the likelihood and cost of being held liable with the immediate cost to invest in controls that may not reduce their exposure.



rate exceeds one percent. As well, the European Union's General Data Protection Regulation (GDPR) uses financial penalties to shift organizational behavior toward data protection.<sup>20</sup>



## Solution Challenges

The challenges to effectuating legal mechanisms (e.g., enacting legislation and establishing judicial precedent) that incentivize cyber risk-reducing behavior are nontrivial, yet the impact of law as a behavioral forcing function is formidable. Relating to the aforementioned gaps, litigation outcomes that may potentially incentivize better security fail to do so because of legal reasoning that dismisses inadequate security-related claims against organizations on the grounds that victims' anticipated harm and resulting protective actions fail legal thresholds.<sup>21</sup>

This trend exposes incongruity between the application of certain laws and the reality of how cybersecurity risk is born out. For example, when sensitive confidential and identifiable information is stolen or lost as a result of a malicious hack or negligent handling, harmful disclosure and use can be very difficult to evidence. Spatially, the electronic data can exist in many places virtually anywhere within the reach of the internet and proving a causal connection can be nebulous. On a temporal level, the harmful 'liquidation' of the identity data (e.g., opening up a new credit account) may not be manifest for weeks, months or years.

From the standpoint of propagating successful models of legally-induced risk transfer, unequal bargaining power between organizations doing business may impede the ability to contractually require vendors to purchase cyber insurance policies or take ownership of the risk via contract.

## Research Objectives

- Evaluate the potential effectiveness (fairness, deterrent effect) of transitive liability models on manufacturers, developers, integrators and other vendors of insecure devices/software
- Study how existing product liability frameworks may be applied to address cybersecurity failures in the context of increasingly connected networks and devices, for example in the automotive, medical, and building controls sectors
- Develop new models and interpretations of traditional product liability theories to adjudicate claims arising from injuries caused by insecure devices
- Explore the role of liability in encouraging organizations to internalize significant negative externalities associated with its activities
- Perform 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 deficiencies
- Investigate the contours of a liability safe-harbor or immunity framework that would incentivize effective cybersecurity, while not dampening innovation
- Develop economic models to quantify the costs to society and individuals relative to organizational gains in situations where exploitation of a common resource causes significant negative externalities

<sup>20</sup> The GDPR can exert fines in the amount of 4% of global revenue or \$20M euros (whichever is larger) for companies who violate its data protection standards.

<sup>21</sup> I.e., victims cannot prove damages or establish legal standing to bring a lawsuit.



## THEME 2:

# ROLE OF GOVERNMENT, LAW, AND INSURANCE

- Develop accountability mechanisms for shared responsibility environments
- Model social and citizen-consumer risk as a factor in quantifying negative externalities
- Identify principles to guide adaptations of applicable laws to new technologies and services that may increase cyber risk exposure; apply the principles to key issues related to “damages” and “harm” caused by new technologies such as liability assignment (e.g., identification of the liable entity, exclusive/joint liability, the role of mandatory or voluntary insurance to cover the liability risk), the nature of liability (fault/non-fault based), burden of proof, and redress possibilities for insurance providers to recover compensated damage

## THEME 3

# THIRD PARTY RISK





## THEME 3:

# THIRD PARTY RISK

### AREA 8 – SUPPLY CHAIN ACCOUNTABILITY

Approaches for improving accountability for security within complex supply chains

#### Current Gaps

There is growing support for the contention that supply chain actors – manufacturers, service providers, developers, integrators – should bear the costs imposed by insecure devices to ensure that suppliers take adequate precautions to prevent destabilization of the internet infrastructure, as well as broad-scale harm to individuals and organizations. 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. Component and system manufacturers lack techniques to account for cyber risks induced by technologies supplied by third parties, and there is no legal/regulatory framework for assigning transitive responsibility.

There is growing support for the contention that supply chain actors – manufacturers, service providers, developers, integrators – 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.

Most discussion of liability assignment in the cybersecurity context has focused on either software [51] or, more recently, the emergence of the IoT (e.g., [52]), where responsibility for connected devices and networks provided by multiple parties is untested and resides within the prevailing legal framework for liability. Direct liability of data holders has been examined (e.g., [53]), with some research (e.g., [54]) indicating that legal liability is unlikely to be a useful mechanism for encouraging better cybersecurity. Without corroboration from further experience, research and analysis, it is hard to foresee how robust these approaches are.

The 2018 DHS Cybersecurity Strategy also reflects on the challenges facing developers and manufacturers to get their products to market rapidly, often at the cost of strong security. It identifies the Department's approach moving forward, shifting incentives towards improved security, both in products themselves as well as in manufacturing and distribution supply chains.

#### Solution Challenges

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 the 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, data flow transparency) to reduce cyber risk.





As well, post-hoc analysis of breach failure points often requires exhaustive forensics that can be inconclusive. In complex networks, it is also possible for harm to arise from a confluence of individual factors that themselves would not be considered reflective of a lack-of-care. Legal treatment of such situations remains unclear. Notably, the increasing proliferation of artificial intelligence (e.g., machine learning, deep learning) and autonomous systems that both comprise and drive modern business introduce a wholly new set of challenges to understanding let alone tracking, explaining and evaluating risk and accountability.

Modern cyber risk contexts characterized by software defects and insecure devices expose loopholes in the traditional product liability regime – strict liability, negligence, breach of warranty. This is primarily due to the economic loss doctrine which bars recovery for productivity loss, business disruption, and other common damages caused by software defects. As well, the application of design defects principles to software is difficult given the complexity of the devices and recent tort reform trends that have limited liability.<sup>22</sup> Further, the intervening cause of damage from insecure software is typically a criminal or tortious act by a third party, so principles of causation might limit liability for manufacturers.



## Research Objectives

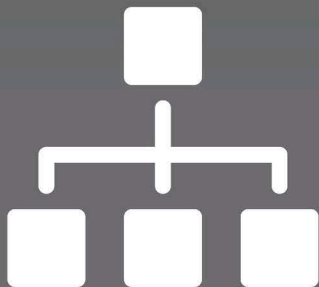
- Model incentives and mechanisms for up- and downstream suppliers (devices, applications, platforms, networks, services) to cooperate to improve cybersecurity
- Understand and quantify how coordination costs factor into shared security contexts
- Understand how exposure to liability in complex supply chains changes behavior, investment, and outcomes
- Assess the extent to which the provisions of existing product liability laws are adequate to solve issues of liability for new technologies and services in complex supply chains
- Evaluate how risk to data propagates in mergers and acquisitions, especially older data originally collected by organizations that no longer exist but that remain sensitive
- Analyze alternative interpretations/applications or legal theories to hold device manufacturers, service providers, integrators, software developers, and end users bear the appropriate costs imposed by design, development, deployment, and uses of technologies that increase systemic or entity-level risk exposure in order to ensure that stakeholders in the supply chain take appropriate responsibility
- 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 audit capability to enable manufacturers to reliably certify the security of components when choosing among prospective suppliers
- Understand which technologies and how their deployments drive third-party risk
- Analyze, model and develop mechanisms for monitoring third party risks in complex supply chains, e.g., contract clauses and policies for the IoT

<sup>22</sup> The most significant hurdles to insecure products liability claims in the IoT are: (1) the application of the risk-utility defect test; and (2) the reasonable foreseeability of the harm under a proximate cause analysis. Many of the risks posed by insecure devices could be mitigated by imposing a post-sale duty to patch vulnerable software, though legislators have so far been hesitant to impose such regulations on software vendors.



## THEME 4

# ORGANIZATIONAL BEHAVIOR AND INCENTIVES



## THEME 4:

# ORGANIZATIONAL BEHAVIOR AND INCENTIVES



## AREA 9 – ORGANIZATIONAL EFFECTIVENESS

Evaluation of the organizational characteristics associated with effective cybersecurity

### Current Gaps

Organizations exhibit great variability in security posture. Much of the variance is owed to diversity in implementation of hard controls, differences in endogenous vulnerabilities, and exogenous factors such as the dynamic actions of attackers. There is a lack of broader understanding of how investments in soft controls mitigate cybersecurity risk. Also in short supply are socio-technical models for identifying and correlating behavioral (individual, organization, social), economic, and technical factors that can affect security performance.

The roles of culture and management are underestimated factors.

The security impact of organizational attributes related to culture and management is often underestimated. Most research on organizational effects is limited to the healthcare sector (e.g., [55][56]). There has been little attention paid to the role of cognitive biases in individual decision making by executives or security operations staff in the context of cybersecurity. Recent research suggests cognitive biases may have a significant effect on cybersecurity professionals (e.g., [57]). While individuals can be influenced to share private data (e.g., [58]), we do not know how they may be influenced in formal professional contexts. Organizations have been shown to suffer the same sort of biases as do individuals (e.g., [59]), but we do not understand the mechanisms by which this behavior morphs from individuals to organizations, and how this can be exploited to weaken or improve security.

### Solution Challenges

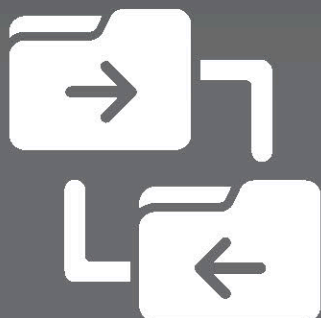
The effect of organizational culture and soft controls can be hard to isolate from that of hard controls. Accurate estimates of individual behavior within “live” organizational settings are challenging. Organizational characteristics outside of firmographics (industry, size, etc.) are harder to measure, though some relatively novel research and industrial offerings are fostering organizational security risk-scoring, based on inferences of risk using publicly-available data (e.g., [60][61]).

### Research Objectives

- Map how incentives at the organizational level get translated to individual cyber risk-reducing behavior; and, identify individual incentives that lead to better organizational performance
- Investigate how the cognitive biases often associated with poor decision making can be exploited to improve behavior
- Assess the relative value of security and risk culture in an organization versus security controls
- Identify the conditions under which automating decisions and actions is beneficial for reducing cybersecurity risk and when is it not
- Develop methods for evaluating processes and capabilities that lead to organizational resilience
- Develop models for integrated cybersecurity expenditures by organizations – where spending for cyber insurance for risk transfer can be considered and balanced with other aspects of cybersecurity behavior such as avoidance, acceptance, and mitigation in order to optimize risk management strategy

## THEME 5

# DATA COLLECTION AND SHARING



## THEME 5:

# DATA COLLECTION AND SHARING



### AREA 10 – INFORMATION ASYMMETRIES

Identify how information deficiencies and asymmetries in the ecosystem affect risk, behavior, decisions, and outcomes

#### Current Gaps

The effects of information shortfalls on risk, behavior, decisions, and outcomes have been extensively considered in the research literature. For example, the cybersecurity market is subject to unreliable disclosures, by which organizations are incented to underreport damage from cyberattacks for reputational reasons, while vendors of security technology are incented to exaggerate the likelihood and severity of attacks [62]. As well, the issue of asymmetric information has been extensively modeled, from a theoretical perspective, for cyber insurance (e.g., [44][45]). Much of the actual empirical research in this area uses data collected during experiments conducted with consumers to understand their behavior and decision making in situations of information asymmetry (e.g., [63]). Less is known about these empirical effects outside this consumer context. Theoretical arguments have led to the somewhat widely held belief that the market for controls is subject to the market-for-lemons phenomenon<sup>23</sup> (e.g., [62]), though more recent empirical work suggests that information sharing among CISOs reduces the impact of market-for-lemons type information asymmetries [30].

The effects of shortfalls on risk, behavior, decisions, and outcomes have been extensively considered in the case of consumers, but less is known about the empirical effects outside the consumer context.

#### Solution Challenges

Much of the research on the impacts of information asymmetries is theoretical because information effects can be hard to isolate, measure, and analyze in the real world. The complexity of decision making environments makes it difficult to determine the bases upon which decisions are made and the role played by asymmetric information versus other factors. 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.



#### Research Objectives

- Provide policy makers, regulators, and other decision makers with an empirically-based analysis of the impact of inadequate information sharing on the cyber risk exposures in specific contexts
- Examine how information deficits affect cybersecurity risk management
- Apply existing and/or devise new techniques to incentivize sharing of sensitive information about specific cyber incidents and trends to inform more accurate predictive risk models
- Measure and expose underlying assumptions and hidden uncertainty across the broad range of cybersecurity risk analyses using innovative techniques, e.g., apply machine learning tools and advanced algorithms to price insurance for specific and systematic risks

<sup>23</sup> A “market for lemons” is thought to arise in situations in which there is no effective way for sellers to demonstrate the quality of their products to potential buyers because buyers cannot distinguish high quality cyber security products from low quality “lemons”. This situation eliminates the price premium that high-quality sellers can earn and causes them to leave the market altogether. When this happens, all remaining vendors are of low quality.



## THEME 5:

# DATA COLLECTION AND SHARING

### AREA 11 – DATA COLLECTION AND MAPPING

Development of tools for efficient and systematic collection of cyber environmental data, and correlation/translation to business-centric data<sup>24</sup> and metrics

#### Current Gaps

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 by the most interesting and significant capability gaps. For example, there is considerable research surrounding data breaches because of the relative availability of breach data (variable quality notwithstanding), while there is very little on control performance. Organizations may be willing to share control performance information, yet efforts targeting this R&D-enabling data have been few and far between.

Current research reflects a reality in which efforts may be disproportionately dictated by data availability rather than the most interesting and significant capability gaps.

Data from a variety of categories and sources are needed to create a more comprehensive picture of both organizational and systemic risk exposures. Greater detail and quality of data are needed with respect to: (1) internally-measured data on threats and vulnerabilities, from organizations themselves or via a third-party service provider with inside access; (2) externally-measured data on threats and vulnerabilities from outside of an organization from publicly-observable viewpoints; and (3) business, financial, or insurance claims data about costs related to loss, damage and/or harm. Several aspects of this comprehensive viewpoint are being addressed currently, at least in part. For example, private sector threat intelligence platforms<sup>25</sup> enable inter-organizational aggregation, correlation, and analysis of threat data. Other commercial and non-profit entities provide externally-observable breach and vulnerability information.<sup>26</sup> The DHS S&T Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) program uniquely coordinates and develops real-world data and information sharing tools, models, and methodologies for cybersecurity R&D. IMPACT makes these resources freely available to stakeholders within the industrial, academic, and government cybersecurity communities [65].

Though the number and scope of data resources is increasing, as the 2016 Federal Cybersecurity R&D Plan points out, “research” in cybersecurity requires realistic experimental data which emulates insider threat, external adversary activities, and defensive behavior, in terms of both technological systems and human decision making... Special, one-off relationships with industry partners to acquire access to their proprietary data means that a broader pool of researchers cannot utilize the data or peer review the results...There is a substantial lack of vetted, provenance -detailed, and openly available data sets that are needed in order to obtain research reproducibility [4].”

<sup>24</sup> Data related to users, networks, devices, software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks [64].

<sup>25</sup> For example, ThreatConnect, EclecticIQ, and Symantec DeepSight.

<sup>26</sup> For example, Identity Theft Resource Center, Privacy Rights Clearinghouse, U.S. Department of Health and Human Services Office for Civil Rights Breach Portal, Vigilante.pw, US-CERT, Census IO, Shodan, etc.





What is in short supply are real-world, large-scale, longitudinal and real-time, heterogeneous, multidimensional, and dynamic datasets needed to enable advances in cybersecurity defenses commensurate with evolving threats [66].

## **Solution Challenges**

Most existing data capabilities are insufficient to address the risk analysis, risk management and decision support needed by enterprise owners and operators across the Federal Government and private sectors. As highlighted elsewhere in this document, there are both widespread disincentives and lack of incentives to share data. The actual and potential data sources are varied and diffuse, rendering semantic fusion and interoperability challenging but necessary. With respect to describing security risk some common language is emerging,<sup>27</sup> but lack of shared definitions limits correlation and synthesis of risk measurements. For example, the meaning of “incident”, “attack”, “breach”, and “event” are not defined in a consistent manner across everyone or even the majority of those who use them; neither then are the attendant metrics and measurements. Given the dynamic nature of many cybersecurity threats, some data have short shelf-lives, putting that much more pressure on efficient collection and dissemination in some contexts. Where data exist, they often have a number of limitations, including proprietary access, high cost, bias in coverage or measurement, or are encumbered by legal and ethical risk. In the long run, reducing asymmetries will require more sophisticated, but not necessarily complicated, data sharing models and implementations that take into account a data needs profile (who, what, when, where, and how) with provable protections for data sensitivities.



## **Research Objectives**

- Catalog data assets, needs and requirements for fusing data across sectors and domains: cyber-logical, cyber-physical, cross-domain, economic, behavioral, societal, and environmental data to address specific cybersecurity challenge problems
- Build and make available scalable and sustainable data assets for government, researchers, and industrial use in cybersecurity evaluation and decision making
- Collect and analyze empirical data that maps actual experience with specific cybersecurity controls to impacts and outcomes in order to build better models
- Define schema to facilitate sharing of high level data such as asset losses and damages
- Develop and implement pragmatic mechanisms for desensitizing data and for linking and sharing disparate sensitive data
- Augment the DHS S&T IMPACT resource platform 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
- Develop practical and sustainable multi-stakeholder mechanisms to responsibly disclose data between law enforcement, industry and research communities
- Empirically model incentives and ROI for cybersecurity data sharing
- Measure the relative value of data sharing in different contexts

<sup>27</sup> For example, VERIS is the Vocabulary for Event Recording and Incident Sharing. It comprises a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner.

## THEME 6

# THREAT DYNAMICS





## THEME 6:

# THREAT DYNAMICS



### AREA 12 – ADVERSARY BEHAVIOR AND ECOSYSTEM

Understanding the behavior and decision making of attackers

#### Current Gaps

Effective defense requires knowledge of attacker processes, incentives, and strategies, and this area has attracted recent attention. Researchers have examined, for example, search-engine poisoning (e.g., [67][68][69][70]), WHOIS misuse (e.g., [71]), distributed denial of service attacks (e.g., [72]), distribution of unwanted software (e.g., [73][74]), the role of consumer credit card-based payment networks (e.g., [75]), affiliate marketing abuse [76], malicious browser extensions [77], fraudulent online pharmacies [78], and financial malware (e.g., [79]). The following deficiencies exist in our ability to address deliberate threats originating from a variety of sources such as national governments, terrorists, organized criminals, hacktivists and hackers:

Effective defense requires knowledge of attacker processes, incentives, and strategies, and while this area has attracted recent attention, going forward it needs to be expanded.

- Model the constantly changing and evolving nature of threats
- Develop models of cybercriminal activity to enable analysis by both security practitioners and social science researchers (e.g., political science, economists, criminologists)
- Examine the attack vectors most likely to be used to significantly disrupt critical infrastructure
- Investigate and model attackers' incentives (e.g., economic, such as profit schemes, tactical, or ideological)
- Develop a common operating picture across relevant stakeholders to assess emerging incidents, threat actors, and associated national, regional, or sector risks

#### Solution Challenges

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. Attack vectors change frequently, at least among the most sophisticated attackers, adding further to the challenge of evaluating the threat. 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. Finally, while cyber criminals are not bound to any rules of law let alone morality, cybersecurity researchers are expected to conform their investigative activities to socially acceptable principles and practices, exemplified in the *Menlo Report* [80] which outlines a framework for ethical guidelines for information and computer information security research.



#### Research Objectives

- Understand how attackers decide on targets and methods for attack
- Develop protection, response, and recovery strategies based on attacker objectives
- Identify intervention points where attack operations are susceptible to disruption
- Understand how implementation of 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 and attack data



# CONCLUSION

---

This research strategy is intended to drive and prioritize research into the business, legal, technical, and behavioral aspects of the economics of cyber threats, vulnerabilities, and implementation of controls. It considers a broad array of research opportunities that will address the Department's cybersecurity goals as well as some of the most pressing gaps in our understanding and capability to address cyber risk. This includes: the quantification of risk; the role of government, law, and insurance; third party risk; organizational behaviors and incentives; data collection and sharing; and threat dynamics. This strategy encourages stakeholders to take a holistic approach to advancements in the area of cyber risk economics, one that incorporates perspectives on managing cyber security from a range of social and behavioral sciences. Such an interdisciplinary approach is essential to improve value-based decision making by those who own, operate, protect, and regulate the nation's vital data assets, functions, and critical infrastructures. Because risk is dynamic and contextual, the relative capability gaps, challenges and research opportunities are expected to change in kind. This strategy is intended to be updated as necessary to help guide progress.

# REFERENCES

- [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>
- [2] Department of Homeland Security. DHS Risk Lexicon. September 2010. <https://www.dhs.gov/dhs-risk-lexicon>
- [3] 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] The White House, Presidential Policy Directive – Critical Infrastructure Security and Resilience, February 12, 2013. <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
- [5] The White House, Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017. <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure>
- [6] U.S. Department of Homeland Security Cybersecurity Strategy, May 15, 2018. [https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy\\_1.pdf](https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf)
- [7] National Science and Technology Council, Networking and Information Technology Research and Development Program, Federal Cybersecurity Research and Development Strategic Plan, February 2016. [https://www.nitrd.gov/cybersecurity/publications/2016\\_Federal\\_Cybersecurity\\_Research\\_and\\_Development\\_Strategic\\_Plan.pdf](https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf)
- [8] U.S. Department of Homeland Security Cybersecurity Strategy Implementation Plan.
- [9] National Risk Management Center (NRMC). <https://www.dhs.gov/national-risk-management-center>
- [10] Computing Research Association. Four Grand Challenges in Trustworthy Computing: Second in a Series of Conferences on Grand Research Challenges in Computer Science and Engineering, 2003.
- [11] National Science and Technology Council, Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program, December 2011. [https://www.nitrd.gov/SUBCOMMITTEE/csia/Fed\\_Cybersecurity\\_RD\\_Strategic\\_Plan\\_2011.pdf](https://www.nitrd.gov/SUBCOMMITTEE/csia/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf)
- [12] Accenture. “Building Confidence: Facing the Cybersecurity Conundrum.” 2016.
- [13] Liu, Yang et al. “Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents,” USENIX Security, August 2015, Washington, D.C.
- [14] Sarabi, Armin et al. “Risky business: Fine-grained data breach prediction using business profiles,” Journal of Cybersecurity, 2(1), 2016, 15-28.
- [15] NIST Special Publication 800-30 Rev. 1, Guide for Conducting Risk Assessments, September 2012. <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>
- [16] Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, January 17, 2017. <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>
- [17] Zurich Insurance Group, The 2016 Global Risks Report, January 14, 2016. <https://www.zurich.com/en/knowledge/articles/2016/01/global-risks-report-2016>

- [18] Department of Homeland Security. Insurance Industry Working Session Readout Report. July 2014.
- [19] Miura-Ko, et al. "Security investment games of interdependent organizations," 2008 46th Annual Allerton Conference on Communication, Control, and Computing, Urbana-Champaign, IL, 2008, pp. 252-260.
- [20] Johnson, Benjamin et al. "Are Security Experts Useful? Bayesian Nash Equilibria for Network Security Games with Limited Information." In: Gritzalis D., Preneel B., Theoharidou M. (eds) Computer Security – ESORICS 2010. ESORICS 2010. Lecture Notes in Computer Science, vol 6345. Springer, Berlin, Heidelberg.
- [21] Johnson, Benjamin et al. "Uncertainty in Interdependent Security Games." In: Alpcan T., Buttyán L., Baras J.S. (eds) Decision and Game Theory for Security. GameSec 2010. Lecture Notes in Computer Science, vol 6442. Springer, Berlin, Heidelberg.
- [22] Lelarge, Marc. "Coordination in Network Security Games: A Monotone Comparative Statics Approach," IEEE Journal on Selected Areas in Communications, 30(1), 2012.
- [23] Johnson, Benjamin et al. "How many down? Toward understanding systematic risk in networks". Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS) 2014.
- [24] Johnson, Benjamin et al. "The complexity of estimating systematic risk in networks." Proceedings of the 27th IEEE Computer Security Foundations Symposium (CSF), pp. 325–336 2014.
- [25] Department of Homeland Security. National Critical Infrastructure Security and Resilience Research and Development Plan. November. 2015.
- [26] Ponemon Institute, 2017 Ponemon Institute Cost of a Data Breach Study, July 26, 2017. <https://securityintelligence.com/media/2017-ponemon-institute-cost-of-a-data-breach-study/>
- [27] Edwards, et al. "Hype and Heavy Tails: A Closer Look at Data Breaches." 14th Workshop on the Economics of Information Security. Delft University of Technology, The Netherlands. 22-23 June 2015.
- [28] Romanosky, Sasha. "Examining the costs and causes of cyber incidents." Journal of Cybersecurity, 2016, 1-15.
- [29] Herley, Cormac. "The Plight of the Targeted Attacker in a World of Scale." Ninth Workshop on the Economics of Information Security. Harvard University, USA. 7-8 June 2010.
- [30] Moore, Tyler et al. "Identifying How Firms Manage Cybersecurity Investment." 15th Workshop on the Economics of Information Security. University of California Berkeley, Berkeley CA, USA. 13-14 June 2016.
- [31] Freund, Jack and Jones, Jack. Measuring and Managing Information Risk: A FAIR Approach. Elsevier. 2015.
- [32] Yu, Sounil. "Understanding the Security Vendor Landscape Using the Cyber Defense Matrix," SESSION ID: PDIL-W02F, RSA Conference 2016.
- [33] MITRE Corporation. Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Threat Preparedness. 2016.
- [34] Khouzani et al. "An economic analysis of regulating security investments in the Internet," INFOCOM, 2013 Proceedings IEEE, April 2013.

- [35] Gordon, Lawrence A., et al. "Increasing cybersecurity investments in private sector firms." *Journal of Cybersecurity*, 1(1), 2015, 3-17.
- [36] Massacci, Fabio, et al. "Economic Impacts of Rules- versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers." *IEEE Security & Privacy*, 14(3), 52-66, May/June 2016.
- [37] Romanosky, Sasha, et al. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management*, 30(2), 2011, 256-286.
- [38] 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>
- [39] Romanosky, Sasha, et al. "Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk?" 16th Workshop on the Economics of Information Security. University of California San Diego, San Diego CA, USA. 26-27 June 2017.
- [40] Innerhofer-Oberperfler, Frank, and Ruth Breu. "Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study." *Economics of Information Security and Privacy*. Moore, T., Pym, D., and Ionnidis, C. (Eds.). (2010): 249-278, Springer US.
- [41] Schwartz, Galina A. and Sastry, Shankar. "Cyber-insurance framework for large scale interdependent networks," *Proceedings of the 3rd international conference on High confidence networked systems*, pp. 145-154, Berlin, Germany. April 15-17, 2014.
- [42] OECD. *Unleashing the Potential of the Cyber Insurance Market*. February 2018, Paris, France.
- [43] Department of Homeland Security. *Enhancing Resilience Through Cyber Incident Data Sharing and Analysis*. September 2015.
- [44] Eling, Martin and Schnell, Werner. "What do we know about cyber risk and cyber risk insurance?," *The Journal of Risk Finance*, 2016, 17(5), 2016, 474-491.
- [45] Bohme, Rainer and Schwartz, Galina. "Modeling Cyber-Insurance: Towards A Unifying Framework." Ninth Workshop on the Economics of Information Security. Harvard University, USA. 7-8 June 2010.
- [46] Terrorism Risk Insurance Act of 2002 (Pub. L. 107-297, 116 Stat. 2322).
- [47] Department of Homeland Security, SAFETY Act. <https://www.safetyact.gov/>
- [48] California Department of Technology Technology Letter, TL-18-01, Issued March 2018, California Cybersecurity Maturity Metrics. <https://cdt.ca.gov/wp-content/uploads/2018/03/TL-18-01.pdf>
- [49] New York State Department of Financial Services 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies (effectuated August 29, 2017). <https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf>
- [50] Chew, Hanley and Newby, Tyler. "Data Breach Settlements: Why Are They Getting Bigger?," *Legaltech news*, November 12, 2017. <https://www.law.com/legaltechnews/sites/legaltechnews/2017/11/20/data-breach-settlements-why-are-they-getting-bigger>
- [51] August, Terrence, and Tunay I. Tunca. "Who should be responsible for software security? A comparative analysis of liability policies in network environments." *Management Science*, 57(5), 2011, 934-959.

# REFERENCES

- [52] Barrett, Lindsey. "The Internet of Things Impacts Liability, Policy, Laws, Regulation, Standards and Governance," American Bar Association SciTech e-Merging News, Spring 2016.
- [53] Romanosky, Sasha and Acquisti, Alessandro. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives of Ex Ante Regulation, Ex Post Liability and Information Disclosure." Berkeley Technology Law Journal, 24(3), June 2009.
- [54] Fryer, Huw et al. "On the Viability of Using Liability to Incentivize Internet Security." Twelfth Workshop on the Economics of Information Security. Georgetown University, Washington, D.C. 11 June 2013.
- [55] Kwon, Juhee and Johnson, M. Eric. "Security Resources, Capabilities and Cultural Values: Links to Security Performance and Compliance" Eleventh Workshop on the Economics of Information Security. Berlin, Germany. 25-26 June 2012.
- [56] Gaynor, Martin, et al. "Is Patient Data Better Protected in Competitive Healthcare Markets?" Eleventh Workshop on the Economics of Information Security. Berlin, Germany. 25-26 June 2012.
- [57] 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 Netherlands. 22-23 June 2015.
- [58] Acquisti, Alessandro, et al. "The Impact of Relative Standards on the Propensity to Disclose." Journal of Marketing Research, 49(2), 2012, 160-174.
- [59] He, Shu, et al. "Cybersecurity Policies Design and Evaluation: Evidence from a Large-Scale Randomized Field Experiment." 13th Workshop on the Economics of Information Security. Delft University of Technology, The Netherlands. 22-23 June 2015.
- [60] Liu, Yang et al. "Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents," USENIX Security, August 2015, Washington, D.C.
- [61] Sarabi, Armin et al. "Risky business: Fine-grained data breach prediction using business profiles," Journal of Cybersecurity, 2(1), 2016, 15-28.
- [62] Anderson, Ross. "Why Information Security is Hard—An Economic Perspective." Proceedings of the 17th Annual Computer Security Applications Conference (2006), 610-13.
- [63] Leon, Pedro Giovanni, et al. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online." ACM Computer Surveys. Vol 1, No. 1, Article 1. September 2015.
- [64] ITU-T. Series X: X.1205, Data Networks, Open System Communications and Security. April 2008.
- [65] Department of Homeland Security Science and Technology Directorate, Cyber Security Division, Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT). <https://www.dhs.gov/csd-impact>; <https://www.ImpactCyberTrust.org>
- [66] Department of Homeland Security, Science and Technology Directorate Strategic Plan 2015-2019. [https://www.dhs.gov/sites/default/files/publications/st/ST\\_Strategic\\_Plan\\_2015\\_508.pdf](https://www.dhs.gov/sites/default/files/publications/st/ST_Strategic_Plan_2015_508.pdf)
- [67] Leontiadis, Nektarios et al. 2014. "A Nearly Four-Year Longitudinal Study of Search-Engine Poisoning," ACM Conference on Computer and Communications Security Proceedings, pp. 930-941, 2014.



- 
- [68] Nektarios Leontiadis, Tyler Moore, and Nicolas Christin. Measuring and Analyzing Search-Redirection Attacks in the Illicit Online Prescription Drug Trade. In Proceedings of the 20th USENIX Security Symposium (USENIX Security'11), pp. 281-298. San Francisco, CA. August 2011.
- [69] Tyler Moore, Nektarios Leontiadis, and Nicolas Christin. Fashion Crimes: Trending-Term Exploitation on the Web. In Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS 2011), pp. 455-466. Chicago, IL. October 2011.
- [70] D. Wang, G. Voelker, and S. Savage. Juice: A longitudinal study of an SEO botnet. In Proc. NDSS'13, San Diego, CA, February 2013.
- [71] Leontiadis, Nektarios and Christin, Nicolas. "Empirically Measuring WHOIS Misuse," European Symposium on Research in Computer Security (ESORICS), pp. 19-36, 2014.
- [72] Brunt, Ryan et al. "Booted: An Analysis of a Payment Intervention on a DDoS-for-Hire Service," Workshop on the Economics of Information Security. University of California San Diego, San Diego CA, USA. 26-27 June 2017.
- [73] Thomas, Kurt et al. "Investigating Commercial Pay-Per-Install and the Distribution of Unwanted Software," Proceedings of the USENIX Security Symposium, Austin, TX, August 2016.
- [74] Stone-Gross, Brett, et al. "The Underground Economy of Fake Antivirus Software." Economics of Information Security and Privacy III. Schneier, B. (Ed.). (2013): 55-78, Springer New York.
- [75] McCoy, Damon et al. "Priceless: The Role of Payments in Abuse-advertised Goods," Proceedings of the ACM Conference on Computer and Communications Security, Raleigh, NC, October 2012, pp. 845-856.
- [76] Chachra, Neha et al. "Affiliate Crookies: Characterizing Affiliate Marketing Abuse," Proceedings of the ACM Internet Measurement Conference, Tokyo, Japan, October 2015.
- [77] DeKoven, Louis et al. "Malicious Browser Extensions at Scale: Bridging the Observability Gap between Web Site and Browser," Proceedings of Workshop on Cyber Security Experimentation and Test (CSET), August 2017.
- [78] Leontiadis, Nektarios and Hutchings, Alice. "Scripting the Crime Commission Process in the Illicit Online Prescription Drug Trade," 1(1), 2015, 81-92.
- [79] Tajalizadehkhoob, Samaneh, et al. "Why Them? Extracting Intelligence about Target Selection from Zeus Financial Malware." 13th Workshop on the Economics of Information Security. Pennsylvania State University, USA. 23-24 June 2014.
- [80] United States Department of Homeland Security. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. August 2012.



**ONLINE**  
[scitech.dhs.gov](http://scitech.dhs.gov)



**FACEBOOK**  
[Facebook.com/dhsscitech](https://Facebook.com/dhsscitech)



**EMAIL**  
[SandT-Cyber-Liaison@hq.dhs.gov](mailto:SandT-Cyber-Liaison@hq.dhs.gov)



**YOUTUBE**  
[www.youtube.com/dhsscitech](http://www.youtube.com/dhsscitech)



**TWITTER**  
[@dhsscitech](https://twitter.com/dhsscitech)



**PERISCOPE**  
[@dhsscitech](https://www.periscope.tv/@dhsscitech)



**LINKEDIN**  
[dhsscitech](https://www.linkedin.com/company/dhsscitech)