AFRL-RI-RS-TR-2018-192

APPLYING BEHAVIOR ECONOMICS TO IMPROVE CYBER SECURITY BEHAVIORS

Georgia Institute of Technology

AUGUST 2018

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2018-192 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
ROBERT KAMINSKI
Work Unit Manager

/ S /
JAMES PERRETTA
Acting Technical Advisor
Information Exploitation & Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
AUG 2018	FINAL TECHNICAL REPORT	Nov 2015 – Nov 2017

4. TITLE AND SUBTITLE

APPLYING BEHAVIOR ECONOMICS TO IMPROVE CYBER SECURITY BEHAVIORS

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA8750-16-2-0051

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Fariborz Farahmand

5d. PROJECT NUMBER
DHS6

5e. TASK NUMBER
GT

5f. WORK UNIT NUMBER
RI

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, GA 30332-0250

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIG
525 Brooks Road
Rome NY 13441-4505

Dept of Homeland Security
S & T CSD
Washington, DC 20528

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2018-192

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Current systems are vulnerable due to poor cyber security behaviors. The existing quantitative models of cyber risk management and cyber insurance are still based on the assumption and behave according to classical decision theories. The approach includes three major activities: 1) quantitative capturing of heuristics and biases in cyber security. 2) quantifying cyber risks, premiums, and selecting control measures to reduce premiums. 3) Transition to practice, will test, evaluate and demonstrate the efficacy of proposed models and transition results to operational environments using “real world databases” and working with “live” partners who eventually will be adopting the models produced.

15. SUBJECT TERMS
Cyber security behavior, cyber risk management

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Robert L. Kaminski
U	U	U	UU	36	19b. TELEPHONE NUMBER (*Include area code*)

Table of Contents

1.0 Summary

Developing quantitative models that "realistically" describe cyber security behaviors, and presenting tangible incentives (e.g., reduced insurance premiums) to corporate managers to improve the security status of their corporations are the need of the hour. The existing quantitative models of cyber risk management and cyber insurance are still based on the assumption, for normative convenience, that stakeholders are rational economic agents and behave according to classical decision theories. These models have little to do with convincing corporate leaders to improve the security status of their corporations.

The Georgia Institute of Technology, in collaboration with major insurance companies, planned to improve cyber security behaviors and address cyber insurance "anomalies"--cyber insurance purchasing and marketing activities that do not produce results that are in the best interest of corporations at risk—through three major activities:

1. ***Quantitative capturing of heuristics and biases in cyber security***. A reality in the cyber insurance industry is that, in assessing premiums and purchasing decisions on cyber insurance, corporate managers are likely to rest on some limited number of simplifying heuristics (mental shortcuts) rather than extensive algorithmic processing. We planned to quantitatively capture these heuristics.
2. ***Quantifying cyber risks, premiums, and selecting control measures to reduce premiums***. We planned to objectively and subjectively investigate cyber risks. For normative decisions, we planned to use the well-established economic principles of expected cost of the cyber incidents. For descriptive decisions, we planned to use behavioral economic theories (e.g., prospect theory) to capture managers' decisions and present the differences of objective and subjective assessments.
3. ***Transition to practice***. We planned to test, evaluate, and demonstrate the efficacy of our proposed models and transition results to operational environments using "real world databases" and working with "live" partners who eventually will be adopting the models we produce. Our findings, in addition to academic and industry journals, planned to be disseminated through PREDICT repository, and delivering courses to industry professionals.

The results of this effort could benefit cyber security industry in at least two ways:

1. ***Provide tangible incentives to improve cyber security behaviors and corporate risk culture***. Our results could assist corporates to translate technical cyber risk into actionable business terms.
2. ***Support critical infrastructure and US economy***. Our quantitative models could capture how cyber critical infrastructures exist, function, and interconnect in the real world, and help IT managers and insurance carriers and underwriters to better understand the value of critical infrastructures and premiums to restore them.

This document provides a summary of our findings, and open- ended interviews with experts across the US, prior to receiving the stop work order. These experts included insurance commissioners (members of the National Association of Insurance Commissioners), insurers and underwriters (e.g., executives from major players in insurance industry), and corporate executives (e.g., chief information security officers and chief information officers of major corporations) across the country.

2. Related work

This section presents a summary of the related work.

2.1 Cyber Insurance, market, and government efforts

Much of the literature and professional commentary on the subject of cyber insurance is devoted to encouraging organizations to purchase cyber insurance against the eventuality of a data breach (e.g., Anderson and Moore 2007). Government regulation also promotes the purchase of this product. For example, the Securities and Exchange Commission (SEC) encourages publicly traded companies to give a "description of relevant insurance coverage," and, in some situations, requires disclosures regarding past cyber-attacks and future threats (SEC 2011). Cyber insurance generally covers two broad categories of risk associated with a data breach. First, such insurance "covers a business in case of unauthorized access or use of its computer network whether internally or externally." Second, cyber insurance "protects a business that violates privacy laws or regulations that protect data from 'unauthorized eyes."(Glascott and Aisen 2013).

According to National Association of Insurance Commissioners (NAIC 2015), the market for cyber liability insurance is off to a good start and it is expected to grow dramatically over time. However, serious concerns remain about the cyber insurance. For example, "price and concerns about too many exclusions, restrictions and uninsurable risks that inhibit organizations from purchasing a policy" are considered as some key road blocks by many midsize companies (Ponemon 2013). Cyber security practitioners have emphasized the need for "tools to help them understand: what cyber risks will implicate which infrastructure components; which components present the greatest concern from a business interruption perspective; what economic and other consequences might ensue without appropriate cyber risk controls in place; and which controls would likely have the greatest mitigation effect" as the requirement for an effective cyber insurance market (NPPD 2014).

To address the current scope of coverage and the possibilities for the future, DHS's National Protection and Programs Directorate (NPPD) started convening a Cybersecurity Insurance Workshop for representatives of government, academia, insurers, information technology, corporate risk management, and critical infrastructure, including electric utilities, in 2012 (see NPPD 2012). NPPD issued a readout report that identified the types of cyber risks that may be insured, including regulatory responses, network damage, and liability and costs arising out of data breaches, among others. They questioned whether most policies will cover physical damage from supervisory control and data acquisition (SCADA) system attacks but noted that utilities typically insure SCADA systems under standalone cyber policies, and that any physical damage resulting from a successful attack on a SCADA system should be covered by a traditional policy of property coverage. The report also discussed the challenges in finding insurance coverage for business interruption and cyber disasters, such as those that might be caused by critical infrastructure failure, terrorism, or war.

Additionally, NPPD convened cyber-risk roundtables in 2013 and 2014 (NPPD 2013, 2014) in which insurance carriers and critical infrastructure owners/operators comprised a majority of the participants. These meetings focused on a topic that had repeatedly arisen in the prior workshop and in feedback received after the publication of the readout report: how to build more effective cyber-risk cultures as a prerequisite to a stronger and more responsive first-party insurance

market (for example, developing coverage for direct loss arising from business interruption, destruction of data and property, and reputational harm resulting from cyber risk).

2.2 Cyber insurance and risk perception

Bruce Schneier (2008) explains that the first, and most common area that can cause the feeling of security to diverge from the reality of security is the perception of risk, for example in assessing probabilities of incidents and magnitude of the costs. However, existing models of cyber insurance neglect the fact that consumers' decisions about insurance can be affected by distortions in their perceptions of risk and by alternative framing of premiums and benefits (e.g., Böhme and Kataria 2006, Grossklags et al. 2008, Pal and Hui 2013).

The standard story is that risk-averse individuals confronted with sizable hazards will pay a more diversified insurer to bear the risk (Dionne and Harrington 1992). In practice, the story is apparently not that simple. In fact, decision scientists and insurance companies have known for "decades" that consumers do not make these choices rationally. Eisner and Strotz (1961) argued that people pay far more for flight insurance then they should. Kunreuther et al. (1978) demonstrated that people do not buy flood insurance even when it is greatly subsidized and priced far below its actuarially fair value.

The recognition that consumer perceptions and decision processes are imperfect and manipulable could be used to support insurance regulation and prohibition of certain types of insurance. Many demonstrations of these framing effects exist, and there is some evidence that insurance itself imposes its own framing effects --different ways of presenting information that can impact on choices between alternatives-- upon risky choice (Camerer and Kunreuther 1989). For example, revealed risk attitudes, as assessed by a certainty-equivalence lottery, differ when the lottery is described as a gamble as opposed to an insurance policy (Hershey et al. 1982).

2.3 Insurance and expected utility theory

The standard theory of decision making under risk--expected utility theory--is not able to explain the above phenomena. Under expected utility theory, a consumer will buy full insurance if and only if premiums are fair; i.e. equal expected losses (this excludes not taking subsidized flood insurance or buying highly loaded cellular-phone insurance). Also, fitting the demand for low deductibles to expected utility leads to implausibly high degrees of risk aversion (Sydnor 2010). Additionally, surveys of actuaries and underwriters indicate that insurers price policies for ambiguous events, such as earthquakes and leakage of underground storage tanks, higher than would be suggested by expected-utility theory or profit-maximization models (Johnson et al. 1993). These pricing decisions could be due primarily to biases similar to those exhibited by consumers, or they may be explained by other factors such as imperfect capital markets and capacity constraints due to insurers' limited liability (Kunreuther et. al 1993).

To illustrate the issue of the expected utility theory in the context of insurance decision making consider the following example:

Example 1- Expected utility theory in the "context" of insurance decision making
Consider the following two formulations:

Insurance Formulation:
Situation A: You stand a 1 in 100 chance of losing $1,000.
Situation B: You can buy insurance for $10 to protect you from this loss.

Gamble Formulation:
Situation A: You stand a 1 in 100 chance of losing $1,000.
Situation B: You will lose $10 with certainty.

According to expected utility theory both formulations involve a choice between [0.01 U (W_o - 1000) + 0.99 U (W_0)] and U (W_0 - 10), where W_0 represents the current wealth level. However, Hershey and Schoemaker (1980) found that under the insurance formulation, 81% of the subjects preferred situation B, compared with 56% under the gamble formulation. Apparently individuals focus on protective aspects when the situation is presented in an insurance context so that this is perceived as a gain. In the gamble formulation, however, people are more likely to perceive the $10 as a loss. 3.

3.0 Theoretical conclusions

This section presents our theoretical conclusions on various related issues; dynamic decision making, quantitative capturing of representativeness heuristics in estimating probability of cyber security breaches, purchasing cyber insurance applying prospect theory (Tversky, and Kahneman 1992), with status quo as reference point, assessing cyber insurance premiums, and quantitative capturing of affective evaluations in cyber risk assessment.

3.1 Dynamic decision making

One of the conclusions of our discussions with the insurance industry executives and our literature review was that the new emerging information systems (e.g., Internet of Things, IOT) and the *connectivity evolution* underscore the insurance and cyber security industry's need for developing "dynamic insurance policies". This led us to study behavioral theories that can quantitatively capture this dynamism. Decision field theory (Busemeyer and Townsend 1993) which takes a cognitive-dynamical approach to decision making and preferential choice appropriate was identified as an appropriate theory for this purpose.

To see how Decision Field Theory, DFT, can be applied to cyber security decisions, consider the following situation. Suppose that a corporate manager needs to decide about purchasing firewall. The choice is to take a risk (not purchase firewall) denoted action *R*, versus play it safe (purchase firewall) denoted action *S*. Table 1 illustrates some basic ingredients entering into this decision (of course this over simplifies the whole situation, but it is useful in illustrating the model).

Action	Event *g* : corporate protected	Event *b*: corporate not protected
Risk (not purchase firewall)	x_{Rg}: communicate with outside network, keep informed, etc.	x_{Rb}: network failure liabilities, data loss, etc.
Safe (purchase firewall)	x_{Sg}: block malicious software, enforce predetermined rules governing what traffic can flow, etc.	x_{Sb} : slow down system, aggravate users, etc.

Table 1: A Hypothetical Cyber Security Decision

According to DFT, the corporate manager deliberates about this decision by thinking about the various possible events that could happen along with the consequences of each action given that an event occurs. From moment to moment, attention focuses on different good and bad events (shown in Table 1 by event *g* and event *b*, respectively) and consequences associated with these events come to mind. At one moment the corporate manger may remember a report he read in the newspaper that morning which described a cyber breach. The next moment, he may think about the competitor corporations which did not purchase a firewall and did not experience any problems. At each moment, affective evaluations of consequences are considered and compared to produce an advantage or disadvantage for one action over another, called a valence. These valences are accumulated over time to form a preference state. The preference state evolves over time as new comparisons are integrated until the accumulated preference reaches a threshold, determining the choice and the deliberation time.

Figure 1 illustrates this preference accumulation process. The horizontal axis represents deliberation time, say in seconds, and the vertical axis represents the cumulative preference for each action at each moment in time. In the figure the upper threshold is crossed first, leading to a choice of the risk. Alternatively, if the lower threshold was crossed first, then the safe option would be chosen. The time required to make the decision is determined by the time required to reach the threshold.

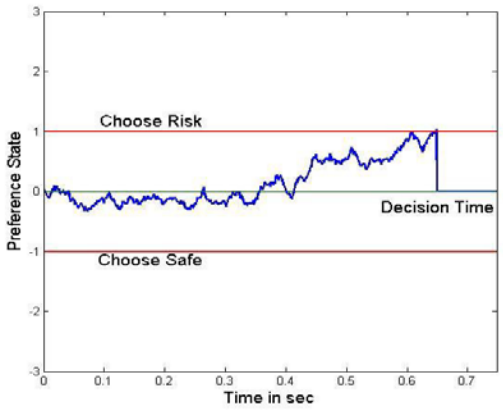

Figure 1--An example sequential sampling process in cyber security decisions

The threshold is an important factor controlling speed and accuracy tradeoffs in cyber security decisions. High thresholds produce decisions based on many evaluations that yield slow responses and high accuracy. Low thresholds produces decisions based on relatively few evaluations, leading

to fast but error-prone decisions. Many factors, such as impulsivity and external time-pressure, may cause the corporate manager to lower his decision threshold. In this way the sequential sampling component of DFT provides an intuitive understanding of many important dynamic aspects of decision-making. Attention to events (e.g., the good event *g* versus the bad event *b* in Table 1) switches back and forth stochastically across time as thoughts are retrieved from memory or stimulated by cues in the environment. This stochastic process modeled as a random walk (discrete time) or diffusion (continuous time) process. Define $P(t)$ as the preference for taking the risk over the safe action state at time *t*, define $v(t)$ as the valence input at time *t* (i.e., the advantage or disadvantage associated with the risky action for the event being considered at time *t*), and define $P(t+h)$ as the new preference for the next time step. Then the preference accumulates according to linear stochastic difference equation $dP(t+h) = P(t+h) - P(t) = -\gamma \cdot h \cdot P(t) + v(t+h)$. The stopping rule is to continue sampling until either $P(t) > \theta$ in which case the risk is chosen, or $P(t) < -\theta$ in which case the safe action is chosen. As the time step *h* approaches zero, this random walk process converges to a continuous time diffusion process.

The valence input term, $v(t)$ has an expectation $\mu \cdot h = E[v(t)]$ and variance $V[v(t)] = h \cdot \sigma^2$. The mean valence μ is determined from the probability of attending to an event, w_j for event *j*, and the valence v_j associated with that event: $\mu = \Sigma\, w_j \cdot u_j$ which corresponds to a traditional utility model. However, the variance also has a critical role in the theory: $\sigma^2 = \Sigma\, w_j \cdot v_j^2 - \mu^2$.

We also found that prospect theory (Tversky, and Kahneman 1992) can be integrated into decision field theory by defining the utilities u_j used by decision field theory in terms of prospect theories reference point value function, and by defining the attention weights, w_j used in decision field theory by the decision weight function of prospect theory. Essentially, decision field theory provides a way to extend prospect theory into a dynamic and stochastic theory of decision making.

3.2 Quantitative capturing of representativeness heuristics in estimating probability of cyber security breaches

The representative heuristic--corporate managers may estimate probabilities from a subset of information, believing that such information is "representative" of the population of information causes individuals to underweight prior probabilities and overweight posterior probabilities--was identified as an important heuristic that could influence cyber insurance decisions. Here, we briefly explained describe the influence of this heuristic on estimating probability of cyber security breaches (Volkman-Wise 2015).

Let us define $P(D_{t+1})$ the actual probability of a loss due to cyber security breach to occur next year, and $P\ (ND_{t+1})$ as the probability of no cyber breach, then according to Bayes' rule we can define:

$$\ln \frac{P(ND_{t+1}|D_t)}{P(D_{t+1}|D_t)} = \delta_L ln \frac{P(D_t|ND_{t+1})}{P(D_t|D_{t+1})} + \delta_P ln \frac{P\ (ND_{t+1})}{P(D_{t+1})}$$

Where δ_L is the weight a cooperate manager place on posterior probabilities, and δ_P is the weight corporate manager may place on prior probabilities. If the corporate manager is Bayesian, then

$\delta_P = \delta_L$, but if the corporate manager is subject to the representativeness heuristic then we will have: $\delta_P < \delta_L$.

Similarly, we can quantitatively describe the impact of representativeness heuristics on Bayesian updating, that is widely used in information security research and practice as follow. If a corporate manager is aware of a recent security breach, the probability of a security breach in next period $P(D_{t+1}|D_t)$ can be calculated as:

$$P(D_{t+1}|D_t)^{RH} = \frac{P(D_{t+1})^{\delta_P}}{P(D_{t+1})^{\delta_P} + (1 - P(D_{t+1})^{\delta_P}}$$

Where $P(D_{t+1}|D_t)^{RH}$ is the probability estimated by a corporate manager subject to representativeness heuristics, RH. If there is no recent cyber security breach $P(D_{t+1}|ND_t)$ can be calculated as:

$$P(D_{t+1}|D_t)^{RH} = 1 - \frac{P(D_{t+1})}{\left(\frac{P(D_{t+1})}{1 - P(D_{t+1})}\right)^{\frac{1-\delta_P}{\delta_L}}}$$

We can show $P(D_{t+1}|D_t)^{RH} > P(D_{t+1})$, and $P(D_{t+1}|ND_t)^{RH} < P(D_{t+1})$ when $P(D_{t+1}) < 0.5$. This suggests the representativeness heuristics can cause lower estimation of cyber security breach, if it has not been experienced recently.

3.3 Purchasing cyber insurance applying prospect theory with status quo as reference point

One the findings of our discussions with the industry executives, insurance agents, and underwriters was that corporate managers consider cyber security breaches as "rare" losses and are unwilling to insure it, where they are willing to insure moderate risks with highly loaded premiums. Applying our findings from literature review, we use the following example to briefly show how prospect theory can describe this behavior, if the status quo is considered as the reference point for corporate manager. The following methodology can also be applied to the situations where initial wealth, or final wealth are considered as reference point.

Recalling the value function from cumulative prospect theory (Tversky and Kahenman 1992) if p is the probability of the first state, the prospect value for a lottery in a two-state lottery is:

$$V = pv(x_1) + (1 - p)v(x_2)$$

Empirical applications of cumulative prospect theory indicate that the value function can be defined as:

$$V(x) = \begin{cases} x^{\alpha} & if\ x \geq 0 \\ -\lambda|x|^{\alpha} & if\ x < 0 \end{cases}$$

That exhibits diminishing sensitivity for $\alpha < 1$and loss aversion for $\lambda > 1$, approximately $\alpha = 0.88$ and $\lambda = 2.25$.

Denoting loss by L, and initial wealth by W, the state dependent wealth is either W or $W - L$. The corporate manager may decide to a buy coverage, denoting by C, for a premium pC, where p is

the probability of the loss, $0< C < L$. Final wealth equals $W - PC$ if no loss occurs, and $W - Lp(1-p)$ if the loss occurs.

If the corporate manager considers status quo as the reference point, then he perceives a gain of $W - Lp - (W - L) = (1-p)L$ with probability p and a loss of $W - pL - W = -pL$ with probability $1-p$, then utility for taking the insurance will be:

$$V = pv([1-p])C + (1-p)\ v(-pC)$$

Applying cumulative prospect theory value function, we will have:

$$V = p((1-p)C)^{a} - \lambda(1-p)\ |-pC|^{a}$$

For any $C > 0$ then we will have:

$$V > (=, <)0 \iff p > (=, <) \frac{\lambda^{1/(1-a)}}{1 + \lambda^{1/(1-a)}}$$

For a graphical representation please see below Figure 1. Left panel despites the situation where the corporate manager perceives purchasing no insurance is optimal and attain a utility level of zero if $C > 0$ that leads to $V < 0$. So, we will have $C = 0$ for $p < \lambda^{1/(1-a)}/(1 + \lambda^{1/(1-a)})$. The right panel shows the situation where purchasing insurance is perceived optimal where $p > \lambda^{1/(1-a)}/(1 + \lambda^{1/(1-a)})$. Here the indifference curve is concave since $V > 0$ and, purchasing cyber insurance coverage is perceived optimal.

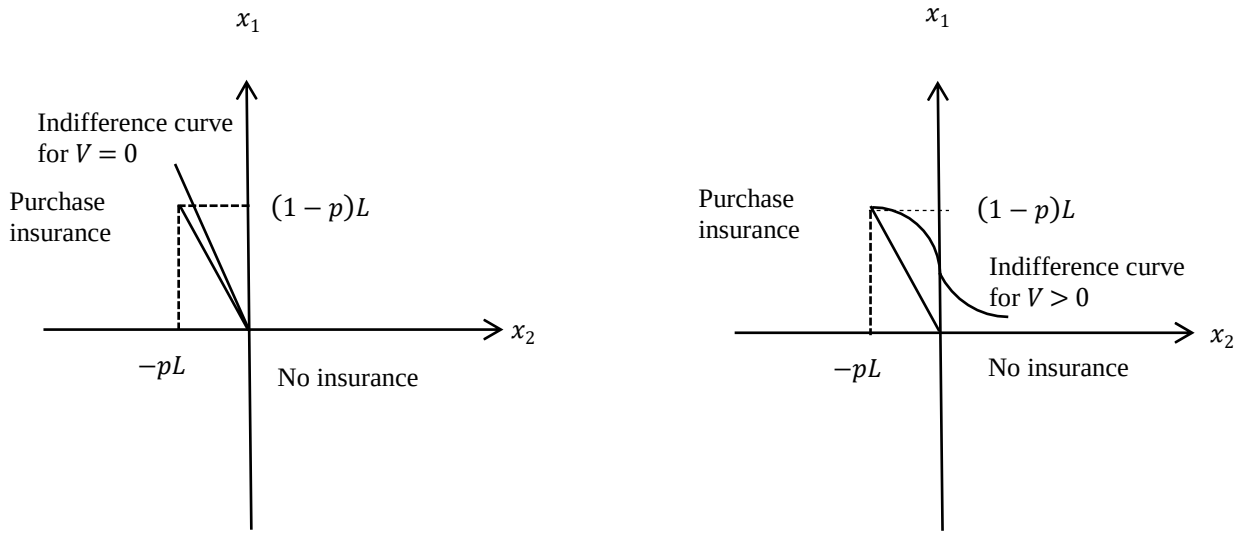

Figure 2: Purchasing cyber insurance with status quo as reference point

3.4 Assessing cyber insurance premiums

The insurance industry has two standard ways of determining insurance premiums: 1) actuarial data, and 2) normative standards. With actuarial data, insurance companies and underwriters are looking at past events to determine how likely they are in the future, e.g. car insurance. With normative standards, insurance companies base their calculations on causal relationships between various factors, e.g. relationship between smoking and cancer in health insurance. Both ways ultimately indicate to the insurance company how likely a loss event is, and the lower the likelihood, the lower the premium for the policy.

However, we find that neither of the above standard approaches is currently being applied in assessing cyber insurance premiums. Fast-paced nature of the use of cyber technologies, issues with quantifying the cost of cyber security incidents, and lack of robust actuarial data are examples of reasons for the inapplicability of these standard approaches in cyber insurance industry. In the absence of standard approaches, we find that cyber insurers and underwriters are left to their own underwriting styles, and their "interpretation" of the results of online questionnaires, on-site audits, previous documentation, and interviews. As such, a great deal of ambiguity/uncertainty (e.g., in assessing likelihoods of cyber security incidents and their various outcomes) is involved in assessing cyber insurance premiums that "may be as much as $3.25 billion, up from $2.75 billion in last year" (Betterley 2016).

We find that insurers and underwriters react to the high level of "uncertainty" regarding average losses from cyber incidents by setting high deductibles and low maximum coverage, resulting in insurance policies that are of little value to risk managers. This could be one of the reasons that many companies are still reluctant to purchase cyber insurance coverage: "Fifty- two percent of respondents believe their companies' exposure to cyber risk will increase over the next 24 months. However, only 19 percent of respondents say their company has cyber insurance coverage" (Ponemon Institute, 2015).

We can address the above issue by quantitatively capturing these uncertainties that are critical in developing "fair" cyber insurance premiums--i.e., the premiums do "not" exceed the expected loss of the hazard, exclusive of administrative expense, tax or other considerations. Here, we briefly explain the two methodologies that we are considering in quantitatively capturing uncertainties in cyber insurance premium assessment:

Ellsberg and Einhorn–Hogarth's model: This is an anchoring-and-adjustment process in which an initial estimate provides the anchor, and adjustments are made for what might be (Einhorn, and Hogarth, 1985). The latter is modeled as the result of a mental simulation process that reflects two factors: (a) the amount of uncertainty, which affects the size of the simulation, and (b) attitude toward uncertainty, which affects the differential weighting of imagined probabilities (Ellsberg 1961).

In our analysis, we can consider two constructs for the uncertainty in cyber insurance premiums: (a) the amount of uncertainty, which affects the size of the simulation, and (b) attitude (both underwriters, from the supply side, and corporate managers, from the demand side) toward uncertainty, which affect the differential weighting of perceived probabilities. We can use an anchoring-and-adjustment process in which an initial estimate provides the anchor. We can sketch

a model of probabilistic judgment under uncertainty and will use it to predict how 1) corporate managers (demand side), 2) underwriters and insurance firms (supply side), and 3) a control group (e.g., academics, system administrators, etc.) are likely to react toward different degrees of uncertainty in various loss categories described in Technical Report Quarter 2 (e.g., breach of privacy event).

Formally, we can start with an anchor on an initial estimate of the probability. Let p represent the anchor that may be based on past experience. The greater the degree of uncertainty experienced, the more alternative values of the probability are simulated and the larger the weight given to such values in the final assessment. Let the adjustment to the anchor be represented by k so that the assessment of the ambiguous probability, denoted $S(p)$, is given by: $S(p) = P + K$. To allow for the effects of ambiguity, we can decompose K into two parts that capture positive (weight given to possible values of the probability above the anchor and is taken to be proportional to (1-P), and negative adjustments, (weight given to possible values below the anchor and is proportional to P). We define θ, a constant of proportionality, that represents the amount of perceived ambiguity where $0 \leq \theta \leq 1$. To account for the fact that values above and below the anchor may be differentially weighted in imagination, θ_p is adjusted to the form θ_p^{β} where β represents the underwriter/corporate manager's attitude. These help us to rewrite the $S(p)$equation as: $S(p) = P + \theta[(1-p) - p^{\beta}$. In this model, θ is the perceived uncertainty determines the amount of the adjustment, and β with level of P determines its sign.

Prospect theory weighting function. Here, the central idea is that when underwriters and corporate managers do not have the underlying objective probabilities they weight the value of gains and losses not with the probabilities themselves, but with a nonlinear transformation of those probabilities, and use *uncertainty weights* that resemble subjective probabilities. We will quantitatively capture this behavior by prospect theory weighting function (Tversky and Kahneman 1992).

Formally, in prospect theory the effects of uncertainty on choice are modeled via a *decision weight function*--the value of each outcome is multiplied by a decision weight, which transforms the relevant probability into its impact on the decision-maker. Decision weights represent a distortion that captures the impact of events on the valuation of prospects, not merely the perceived likelihood of those security events.

Prospect theory suggests the following weighting functions to capture the probabilities:

$$\omega^{+}(p) = \frac{p^{\gamma}}{(\,p^{\gamma}+(1-p)^{\gamma)^{1/\gamma}}}$$

$$\omega^{-}(p) = \frac{p^{\delta}}{(\,p^{\delta}+(1-p)^{\delta)^{1/\delta}}}$$

where p is probability of the outcome, and ω^+ and ω^- are the decision weights on positive outcomes and negative outcomes respectively, and measured experimentally by Tversky and Kahneman (1992): $\gamma = 0.61$, and $\delta = 0.69$. A hypothetical weighting function shown in Figure3.

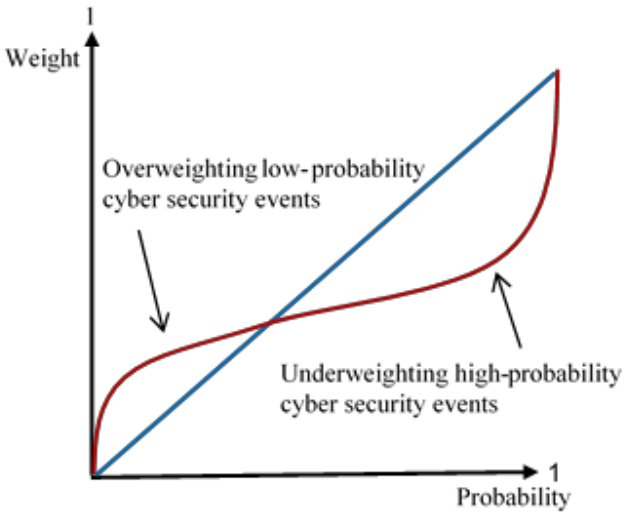

Figure 3- Decision weights vs. actual probability in cyber insurance premium assessment--according to prospect theory

In Figure 3 the curvature of the weighting function explains the characteristic reflection pattern of attitudes to risky prospect.

3.5 Quantitative capturing of affective evaluations in cyber risk assessment

We find that affective evaluation, such as evaluation based on positive and negative prior experiences, can influence one's attitude (both underwriters and corporate managers) toward cyber security risks. We posit that prior experiences can lead to sensitization effects on the shape of the prospect theory utility function, and will empirically investigate it. Formally, the prospect theory value function that defines gains and losses to a reference point is concave in the domain of potential gains, and convex in the domain of potential losses:

$$v = f_{PT}(x - x_{ref}) = \begin{cases} (x - x_{ref})^a, & x - x_{ref} \geq 0 \\ -\lambda(-(x - x^{ref}))^b, & x - x_{ref} < 0 \end{cases}$$

$$0 < a < 1, \qquad 0 < b < 1, \qquad \lambda > 1$$

The prospect theory value function can capture affective valuations and the sensitivity in both domain of gains and losses. For example, when $b > 1$ (concave): risk averse, when $b = 1$ (linear): risk neutral, and when $0 < b < 1$ (convex): risk seeking. Figure 4 despites the shape change of the prospect theory value function (blue curve) under negative prior experiences (red curve). For example, experiencing a breach of privacy can change his risk attitude toward subsequent losses. This change would steepen the utility curve in the gain domain ($V'_G > V_G$) and flatten it in the loss domain ($V'_L > V_L$).

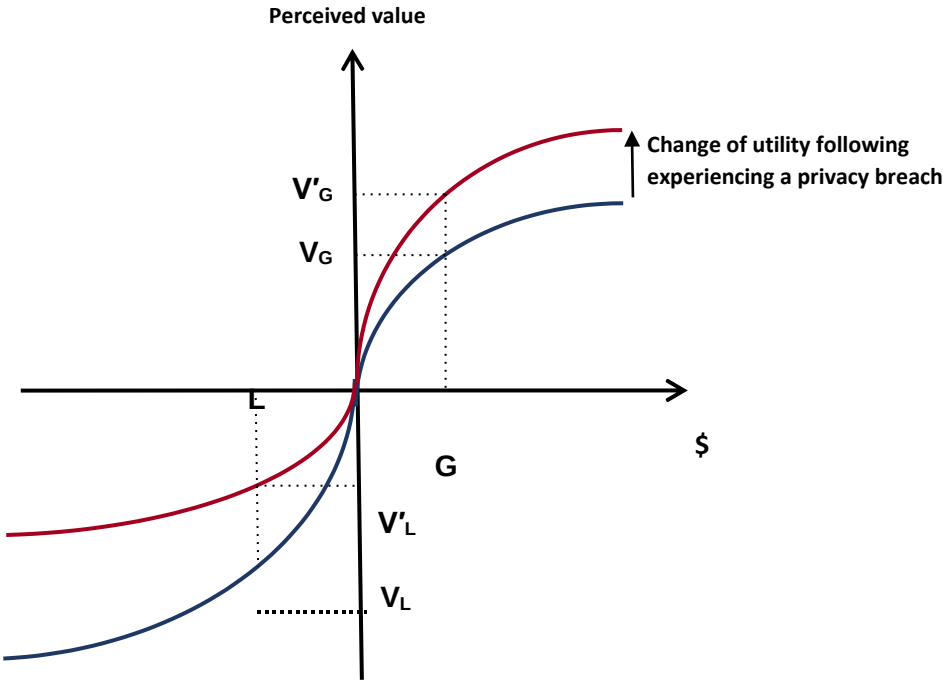

Figure 4—The impact of negative prior experience on prospect theory value function

4.0 Discussions with experts

The section highlights a summary of our discussions with experts (insurance commissioners, corporate executives, insurers, and underwriters) who participated in our discussions. For convenience, summary of the statements made by the interviewees are in italic.

4.1 capturing ambiguities in measuring premiums

An expert stated: "*We understand the concepts and definitions in NIST Framework. But, at the end of the day, we need to measure primiums. The problem with applying the Framework is that we get very different numbers from different experts, even in one division of our company. These ambiguous risks are quite problematic for us. In our business, the more ambiguous the risk is, the less likely an insurer will offer it on the market. Or, if they offer they charge a very high price to make it worth their while. Can your work help us understand reasoning of individuals and groups faced with ambiguous risks? Does your work present a formal methodology that our technical folks can follow?*"

Prior to providing a summary of our answers, we would like to point out that these experts' statements about the NIST Framework are consistent with our findings from the literature review. As an example, here is a summary of a case study by Intel (Intel 2015). In this case study, Intel performed an initial high-level risk assessment on the office and enterprise environments. Three groups of subjects were involved in the Intel case study: 1) core group, including 8 to 10 senior

security subject matter experts, SMEs, and mid to- senior-level security capability or program managers, who set target scores, and performed an initial risk assessment and scoring, 2) individual security SMEs, who scored the risk areas, and 3) stakeholders and decision makers, who approved target scores, reviewed assessment results, and set risk tolerance levels. The results of this study indicated "significant differences between core group and individual SME scores can identify visibility issues, either by the individual SME or the core group".

4.2 Insurance premium decisions under uncertainty

Here, first, we explained prospect theory and support theory in *lay terms,* and how these theories distinguish between events in the world and the manner in which they are mentally represented. For example, probabilities are attached not to events, as in standard normative models, but rather to descriptions of events, and probability judgments, are based on the support (strength of evidence) of the focal hypothesis relative to that of alternative. We provided simple real life examples of how these theories distinguish between explicit disjunctions that list their individual components, and implicit disjunctions which do not; ''a car wreck due to road construction, or due to driver fatigue, or due to break failure, etc.'' vs. "a car wreck".

Then, we explained how different presentations of an event can lead to different measurements of premiums. For example, *unpacking* a description of an event into disjoint components (i.e., from an implicit to an explicit disjunction) generally could increases its support and, hence, its perceived likelihood. That is, it brings to mind neglected possibilities or by increasing the impact of unpacked components. As a result, different descriptions of the same event can give rise to different judgments.

Following this description the interviewees were able to explain to provide their own examples of unpacking: "*so, willingness to take protective action such as the purchase of insurance might also be increased by unpacking the ways in which a relevant mishap might occur*" or "*when cyber risk components are evaluated separately, corporations which were not interested in purchasing insurance may be actually willing to pay a premium*".

Finally, based on our analysis and literature review, and findings from behavioral economics (Fox and See 2003), we formally explained the two-stage model in which the decision maker first assesses the probability P of an uncertain event A, then transforms this value using the risky weighting function, and presented the flowchart for this process, as shown in Figure 5. In Figure 5, $V(x, A) = v(x)W(A) = v(x)(\omega\ [P(A)])^{\theta}$, where $V(x, A)$ is the value of the prospect that pays $\$x$ if event A obtains (and nothing otherwise), $v(.)$ is the value function, $P(.)$ is judged probability, $\omega\ (.)$is the risky weighting function, and θ is the source attractiveness and inversely relates to the attractiveness of the source of uncertainty.

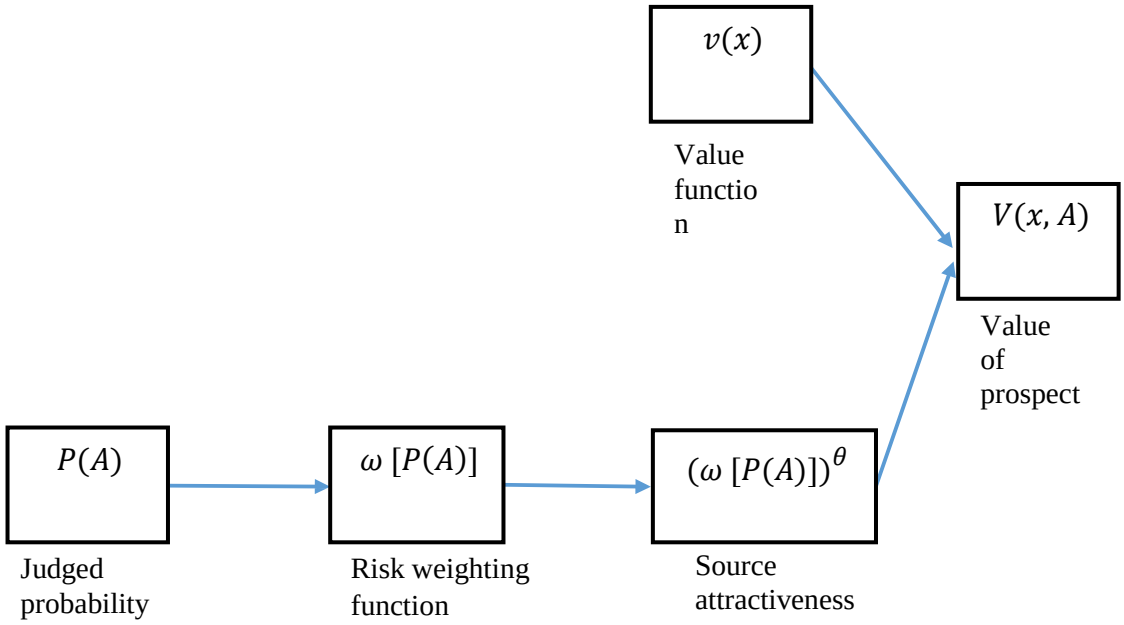

Figure 5- A sample flowchart showing insurance premium decisions under uncertainty

4.3 Illustrating degrees of ambiguity

Here, we started by explaining the concept of utility as values associated with decisions. Then, we explained how our work and behavioral economics (Camerer, and M. Webber 1992) can identify different scenarios about utilities of decisions/actions with a probability *p*, and presented these scenarios, as described below, and shown in Figure 6, next page:

1- *Certainty*. When the decision maker knows one state will occur with certainty ($p = 1$) his/her distribution of *p* is the vertical line shown in figure 6a. This is certainty.
2- *Risk*. When the decision maker is not sure of states, but knows the probabilities of states precisely, his/her distribution is similar to figure 6b. This is risk, or unambiguous probability.
3- *Ambiguity*. When the decision maker is not sure what the distribution of probabilities is, then the probabilities are ambiguous. We consider two kinds of ambiguity. First, when the probability distributions in the set of thinkable distributions can themselves be assigned probabilities, ambiguity can be expressed as second-order probability (i.e., expressing knowledge about probabilities). This is shown in Figure 6c. Second, when the distributions cannot be assigned probability, ambiguity is expressed by a set of probability distributions as the amount or nature of missing information varies. This is shown in Figure 6d.

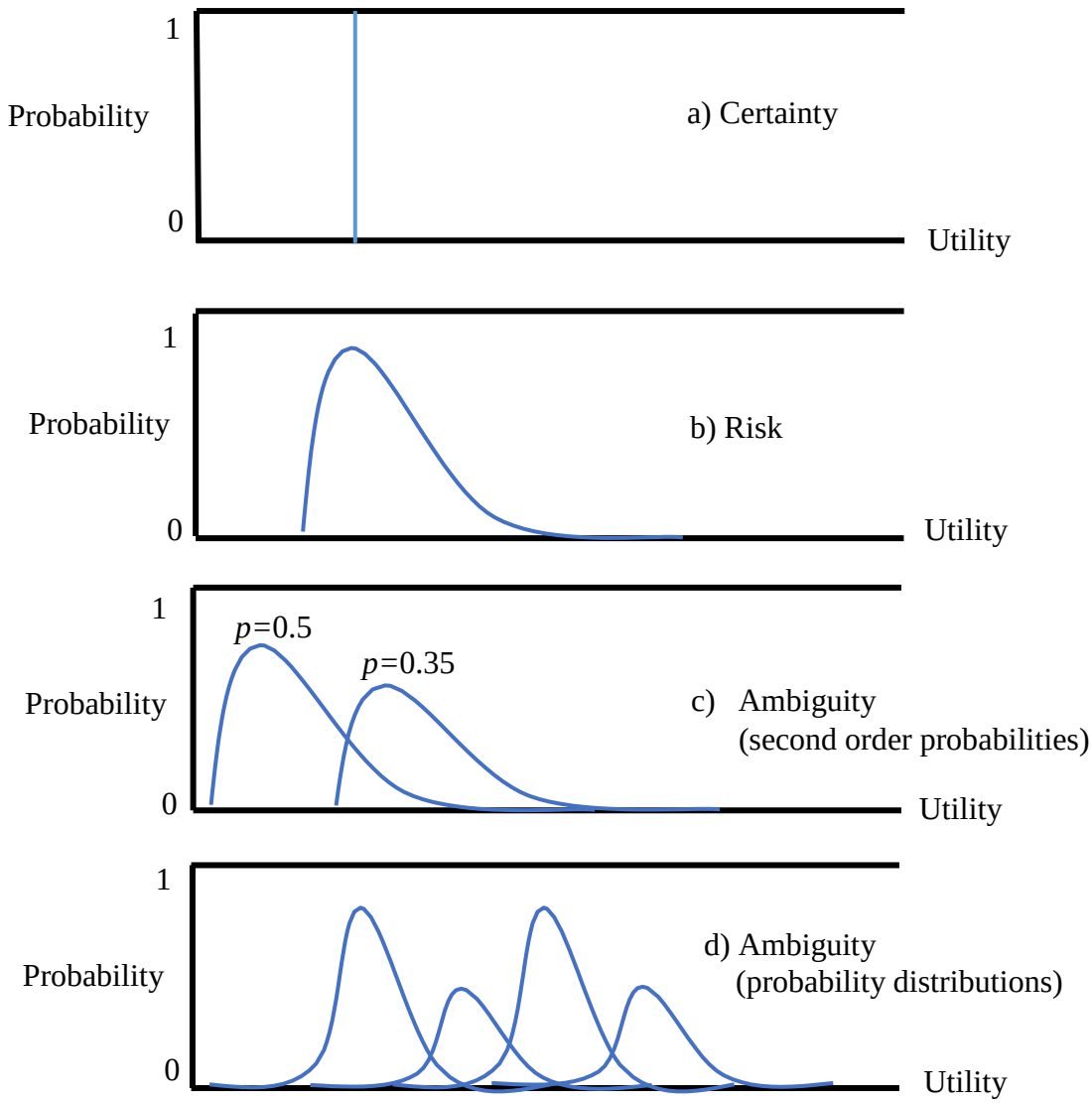

Figure 6- Presentation of insurance premium decisions under risk and uncertainty

4.4 Reservation price and risk appetite

An expert stated: "Underwriters and insurers still don't have measureable, repeatable methods to deal cyber risk and assess premiums, and we are still learning about how companies actually make decisions about cyber risks. But, we do know in many situations they make decisions based on their risk appetite. Can your work on prospect theory help us with understanding different stakeholders' risk appetite? Can you describe your analysis, and results in the form of graphs that we can present in our meetings?"

We found these experts' statements to be consistent with our findings from the literature review, and publicly available statements from senior industry executives, e.g., "I haven't even seen a survey that compares how underwriters are measuring risk and pricing policies today, or how they are hedging the risk assumed, and what kind of reserves are required" (Schutzer 2015). The

experts' statements were also consistent with the recent industry guidelines for purchasing cyber insurance: "While there is some regulatory guidance, much of the determination is dependent upon an organization's risk appetite. This space is still developing and currently there is no authoritative schematic for cyber insurance purchasing" (FSSCC 2016).

Here, following a brief explanation of the law of large numbers, we discussed the concept of *reservation price* for insurance--the maximum amount a consumer would pay for insurance against a loss and can be calculated as: initial wealth - certainty equivalent (Camerer and Kunreuther 1989). We also explained some simple implications of the reservation price. For example, if the cyber insurance premium is cheaper than the reservation price, the consumer will buy the policy, and gain from pooling risks. Then, we briefly explained prospect theory value function, and our formal analysis as follow, and presented Figure 7. We explained, let us assume each party corporation has a reservation price of P_c^*, and insurers has a reservation price of P_i^*. If the corporation can insure and suffer a loss of $v\,(-P_c^*)$ with the probability of r with loss of L, they can proceed with insurance, and have a prospect of $\pi(r)v(-L)$. This (i.e., corporate's reservation price) is shown in Figure 7-a. Similarly, insurer's reservation price can be calculated as $v\,(P_i^*) + \pi(r)v(-L)$, and be presented as in Figure 7-b.

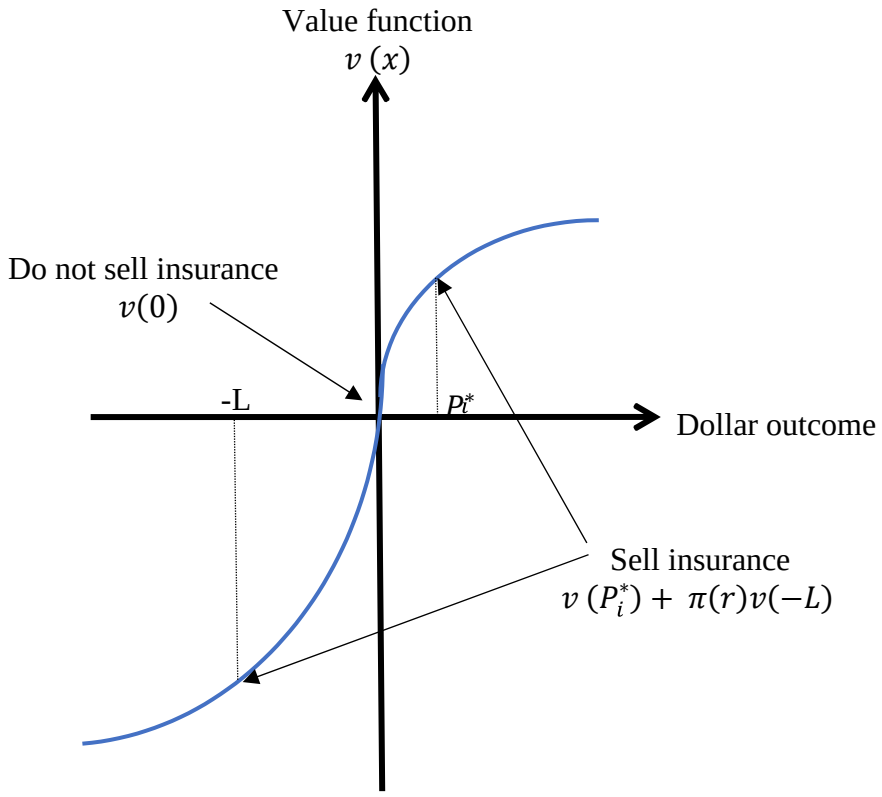

Figure 7a- Corporation's choice using reservation price and prospect theory

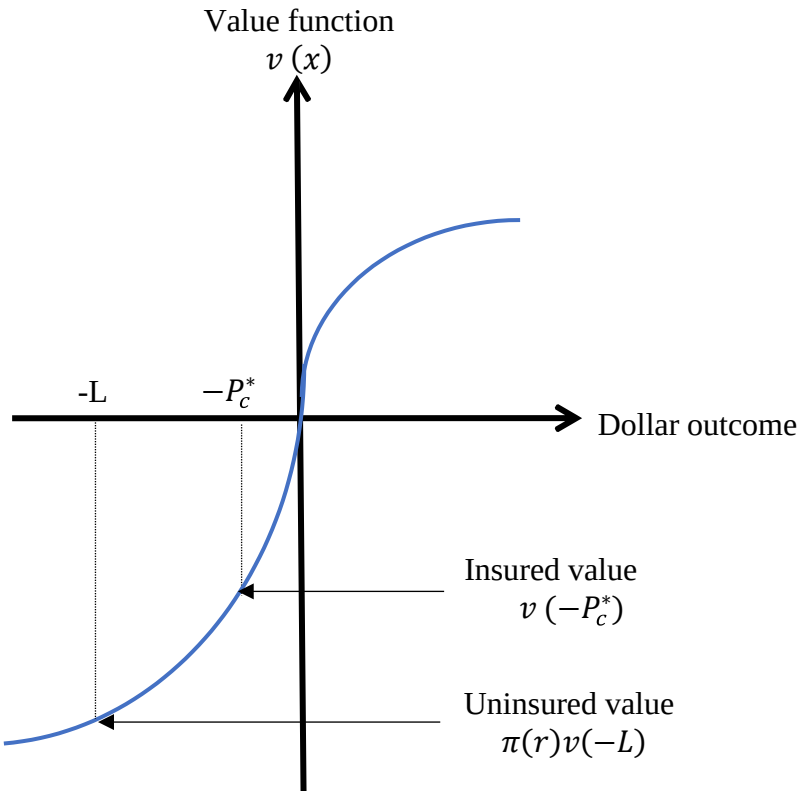

Figure 7b- Insurer's choice using reservation price and prospect theory

4.5 Heuristics and cyber insurance subsidy

An expert stated: We have seen the influence of heuristics and biases in purchasing different types of insurance like flood, and earthquake. But, cyber insurance is a new one. As commissioners, we need to think about protecting consumers in various situations. How can we use your work in understanding subsidization needs and fair premiums, let's say after a cyber disaster? Have you considered these extreme events in your models?

We briefly explained the representativeness heuristics (we have discussed this heuristic in details in previous reports) and the following model, based on our analysis and literature review:

$$P(D_{t+1}|D_t)^{RH} = \frac{P(D_{t+1})^{\delta_P}}{P(D_{t+1})^{\delta_P} + (1 - P(D_{t+1})^{\delta_P}}$$

where $P(D_{t+1}|D_t)^{RH}$ is the probability estimated by the consumer who is subject to representativeness heuristics, RH, and δ_L and δ_P are the weight consumer may place on posterior and prior probabilities, respectively. If the consumer is Bayesian, then $\delta_P = \delta_L$, but if the consumer is subject to the representativeness heuristic then we will have: $\delta_P < \delta_L$. We also explained that the critical loading factor (reflecting the insurer's costs of operating the plan) can be calculated as:

$$\frac{P(D_{t+1}|D_t)^{RH} - P(D_{t+1})}{P(D_{t+1})}$$

Then, we presented graphs describing the above equation and decision weights vs. actual probability in cyber insurance premium assessment, and how and how these can influence the loading factor. We also explained various situations where corporate executives subject to the representativeness underinsure prior to a disaster and over insure post-disaster, and they may purchase unfairly priced policies post-disaster. As such, insurance commissioners should be cautious of the degree to which they allow insurers to increase premiums after a disaster occurs, given consumers' preferences. Such errors in probability estimation may justify subsidization of insurance policies when a disaster has not occurred recently.

4.6 Identifying loss exposure categories for insurance premium assessment

Based on the results of our discussions with the industry executives, underwriters, and publications of insurance brokers (e.g., Marsh), and accounting firms (e.g., PWC), the 17 loss categories mentioned in Table 2 are considered for our risk premium assessment:

Loss category	Example
1. Breach of privacy y event	Cost of IT forensics and notifying affected subjects
2. Data and software loss	Cost of reconstituting data and software
3. Incident response costs	Direct cost to close the incident
4. Cyber extortion	Cost of expert handling an extortion incident
5. Business interruption	Lost profit due to the unavailability of services
6. Multi-media liabilities	Civil damages arising from defamation, copyright/trademark infringement
7. Regulatory and defense coverage	Coverage for fines, penalties
8. Reputational damage	Loss of revenues from future customers
9. Network service failure liabilities	Third-party liabilities arising from security events
10. Contingent Business Interruption	Business interruption resulting from the IT failure of a third party
11. Liability	Coverage for third-party claims relating to failure to provide adequate professional services or products
12. Financial theft and fraud	Damages caused by disgruntled employees
13. Intellectual property theft	Loss of value of IP assets
14. Physical asset damage	Destruction of physical property
15. Death and bodily injury	Liability for death and bodily injuries
16. Cyber terrorism	Damages caused by a foreign government as an act of war or a terrorist attack
17. Environmental damage	Costs of clean up associated with a cyber-induced environmental spill

Table 2-Tentative general loss categories for cyber insurance premium assessment

On the relative importance of loss exposure indicators, we found a wide range of opinions across various industries. We have started defining indicators for insurance underwriting and risk selection under 5 general categories and plan to revise these indicators over time. The five tentative

categories that we are currently considering in this research are: 1) Corporate activities and profile (e.g., business sector, revenue), 2) Risk management process (e.g., incident response plan, employee awareness), 3) Confidential records and data assets (e.g., data shared with third party, intellectual property), 4) Network security (e.g., configuration of network, patching vulnerabilities), and 5) IT security practices (e.g., in-house and outsourced IT services, backup processes and recovery).

4.7 Cyber physical systems, and cyber insurance

We asked the experts to share their experiences, and to express their real-world views on cyber insurance and cyber physical systems (CPS). We had follow-up discussions with experts in microelectromechanical systems (MEMS) and material engineering at Georgia Tech. We also reviewed related academic and industry literature to find the results of the studies (if any) that address the issues mentioned by our interviewees. The following is a summary of our findings.

The currents status of CPS and insurance industry. Many experts, in response to: what problems keep you awake at night?, answered: "CPS risks". One expert stated:

"*We know we are facing major technical challenges in insurance industry. But, frankly, we are far from being prepared for it", are examples of the comments that the PI received in his discussions with the interviewees*.

The need for an "engineering understanding" of CPS risks, "both" at the cyber and physical level (i.e., not just at the cyber level, as it seems to be the focus of majority of ongoing research on CPS), was mentioned by all the interviewees. To shed light on the issue, we provide a summary of a scenario that was described by an insurer, and we shared with other interviewees:

> *"Let us say we have a client who calls us about an issue about his airbag sensor, after a recent car wreck. We can quickly take care of it: we can send our folks to do a point-to-point inspection, disassemble the car if needed, and tell was the issue caused by the wreck, or was it a mechanical failure, and irrelevant to the wreck. We can do this because here the engineering concepts are well understood and we can draw conclusions about the whole system. But, with CPS we don't have an engineering understanding of how the system works. We really don't know how the physical components of these cars are working with the cyber components."*

We shared the above scenario with other experts. Here is some sample feedbacks that were provided:

An executive from the electronics industry said: "*I agree with the insurer's point. To add to his example, with CPS we cannot even tell if that car problem was a MEMS problem, or no it was a material problem, fatigue failure, for example. Currently, we are not even sure which MEMS is the right one for these cars*."

An expert stated:

"*The example is a good one, but in our industry, it is just tip of the iceberg. Telematics has brought many challenges to us. We need to write policies and want to use MEMS to monitor body activities (like vibrations), gas (like smell of alcohol) in the cars. For our new policies, we call it full-behavioral-rating we need quantitative models to analyze the information that are coming from MEMS about all different things that are happening in the car. But, we don't have such models*."

***Implementing NIST frameworks in assessing CPS risks*.** Applicability of NIST frameworks in cyber insurance and CPS was also discussed during our discussions with the interviewees. We find it encouraging that most of them were familiar with the NIST Cyber Framework and interested in applying it in their organizations, and in their work with their clients. However, in request for more details about the actual implementation of the Framework, they only could name some Framework Core Functions (e.g., identify, protect, detect, …) and nothing about Implementation Tiers. Although, they were aware of NIST's intention--"It's a framework, not a prescription" (Barrett 2015) --they believed it would be considerably more effective if they could receive "help assessing risk in a more analytic way". Similar comments were also made about the practical benefits of the models have been developed to use the Framework (e.g., Yu 2016) and the recently released NIST Framework for Cyber-Physical Systems (NIST 2016).

Review of academic and industry literature. Literature review did not lead to any practical quantitative model to "integrate" information risk assessment (cyber component) with material risk assessment (physical component). But, the literature review indicated the importance of having such models. For example, Amin et al. 2013 explained: "Insurance instruments of CPS risks management are meager: the premiums of cyber-security contracts are not conditioned on the security parameters", and "The main challenge for CPS experimentation on the DETERLab testbed is to compose physical system dynamics (real/simulated/emulated) with communication system emulation."

5.0 Technical comments from the program manager

In the technical comments that we received on Quarter 2 Technical Report (see Exhibit A)--the only technical comments that we received on our technical reports-- it was stated:

> "*Data breaches are one of the few cyber coverages for which insurers have built real actuarials and where they are keen to realize premium profits.*"

However, we did not receive a response from the program manager to our request to review the documents that explain how "…insurers have built real actuarials", and how insures are actually using them in cyber insurance", and to related statements from experts, such as:

> "*In most of the world, steadily accumulating actuarial data and learning from them brings success. In the Internet business world, however, such a strategy is almost impossible…. In the electronic business world, the technical flux of change is high—so high that actuarial data are practically impossible to obtain*" (Geer et al. 2003)

> "*While actuaries do need as much historical data as they can get, past data is not always indicative of future events and their cost. …The challenge is much greater than not having historical data. Because cyber risk is growing and rapidly evolving, information about the past may be of limited direct predictive value when looking at the future.*" (Baribeau, 2015).

We also discussed the program manager's comment with various insurance commissioners, and cyber security practitioners. However, we found many similar statements to those made by Geer et al. 2003, and Baribeau, 2015. The following is a sample statement, made by a senior member of the National Association of Insurance Commissioners (NAIC) (see Exhibit B):

> *"For most products, the insurance industry is able to rely on historical data to assist in pricing for future losses. Not so for cybersecurity insurance products where evidence of a data breach in the past might not be indicative of a future data breach. This is because businesses tend to be more attentive to cyber risks once they have been subject to a breach. Thus all cybersecurity insurance pricing to date is based on an evaluation of the cybersecurity practices of the business seeking to purchase coverage and the judgment of the underwriter as to what price to charge."*

6.0- Insurance premium assessment and selecting control measures

This project received a stop work order while we were conducting a comprehensive literature on the planned task on developing quantitative models for cyber risk assessment, premiums, and selecting control measures to reduce premiums. As such, we could not complete this task, and other tasks of the project that depended on this task. However, we have listed some of the sources that were studying for this task with * in References for future research.

7.0 Conclusions and Recommendations

Our results indicate that in the cyber insurance industry in assessing premiums and making decisions about purchasing cyber insurance, corporate executives are likely to rest on some limited number of simplifying heuristics (mental shortcuts) rather than extensive algorithmic processing. Developing computational models that can realistically describe cyber security behaviors and present tangible incentives, such as reduced insurance premiums, to corporate executives to improve the security status of their corporations are the need of the hour. The existing computational models are still based on the assumption, for normative convenience, that stakeholders are rational economic agents and behave according to classical decision theories. That is, they have little to do with convincing corporate leaders to improve the security status of their corporations.

Our results also indicate that developing actuarial data for cyber insurance require stability of the underlying entity being measured, and such stability does not exist in cyber security data. That is, the existing databases, even those with large volumes of data, could be of little help to cyber insurance practice. In the absence of actuarial data and standard realistic computational approaches, insurers and underwriters are left to their own underwriting styles, and their interpretation of the results of online questionnaires, on-site audits, previous documentation, and interviews. As such, the first step to improve the cyber insurance market, could be narrowing down the scope of cyber expertise required of underwriters by targeting specific industries or niches within them, and identifying specific heuristics that could influence the decisions on specific exposures

As a senior member of NAIC had stated about this research it had “promises to add certainty where only an educated guess exists today. Adding certainty where little exists should also attract more insurance providers who are now watching from the sidelines because they don’t know what to charge”. We hope the future research can continue this effort. Future research on cyber insurance requires collaboration among academia, industry, and government. It needs to address at least two fundamental operational issues in information security market: 1) how can we improve cyber security behaviors? 2) how can we assist corporate executives in dealing with cyber insurance, similar to other types of insurance? That is, accepting some amount of risk, mitigating some more risk with various technologies (e.g., virus scanner) and procedures (e.g., security policy), and insuring the rest of it. This is similar to fire prevention, shoplifting, or any of the other risks that could affect corporations.

References:

*Advisen, *Cyber liability insurance market trends survey*, Advisen Ltd., 2014.

*AIG, Cyberedge cyber liability insurance - policy wording. Technical repor.t

S. Amin, G. A. Schwartz, and A. Hussain, "In Quest of Benchmarking Security Risks to Cyber-Physical Systems," *IEEE Network*, 19-24, 2013.

*C. J. Alberts, and A. J. Dorofee. *OCTAVE Criteria*,Technical Report CMU/SEI-2001-TR-016, CERT, December 2001.

*M. A. Amutio, and J. Candau. *MAGERIT – version 3.0. Methodology for Information Systems Risk Analysis and Management. Book I - The Method*, Ministry of Finance and Public Administration
Technical Secretariat Information, Documentation and Publications Unit Publications Center, 2014.

R. Anderson, and T. Moore, "Information Security Economics—and Beyond", *Proceedings of the 27th annual international cryptology conference on Advances in cryptology*, 68-91, 2007.

*Armic, *Airmic review of recent developments in the cyber insurance market*, Airmic Technical, 2012.

*W. Baer. "Rewarding it security in the marketplace", *Contemporary Security Policy*, 24(1):190–208, 2003.

*W. S. Baer, and A. Parkinson, "Cyber insurance in it security management," IEEE Security and Privacy, 5(3):50–56, 2007.

*D. J. Ball and John Watt, "Further Thoughts on the Utility of Risk Matrices", Risk Analysis, Vol. 33, No. 11, 2013.

A. G. Baribeau, "Cyber Insurance: The Actuarial Conundrum", *Actuarial Review*, Causality Actuarial Society, 42 (4), 33-38, 2015.

M. Barrett, Overview of the Cybersecurity Framework Implementation of Executive Order 13636, January 2015.

*L. Bailey, "Mitigating moral hazard in cyber-risk insurance, *JL & Cyber Warfare*, 3:1, 2014.

*T. Bandyopadhyay, "Organizational adoption of cyber insurance instruments in it security risk management a modeling approach", *SAIS 2012 Proceedings*, 2012.

*T. Bandyopadhyay, V. S. Mookerjee, and R. C. Rao, "Why IT managers don't go for cyber-insurance products, *Communications of ACM*, 52(11):68–73, 2009.

*T. Bandyopadhyay, V. S. Mookerjee, and R. C. Rao. A model to analyze the unfulfilledpromise of cyber insurance: The impact of secondary loss. Working Paper, 2010.

*T. Bandyopadhyay and S. Shidore, *Towards a managerial decision framework for utilization of cyber insurance instruments in it security*. In V. Sambamurthy and M. Tanniru, editors, AMCIS. Association for Information Systems, 2011.

*K. Beckers, L. Krautsevich, and A. Yautsiukhin, "Analysis of social engineering threats with attack graphs", *Proceedings of the 3rd International Workshop on Quantitative Aspects in Security Assurance*, 2014.

*S. P. Bennett and M. P. Kailay, "An application of qualitative risk analysis to computer security for the commercial sector", *Proceedings of 8th Annual Computer Security Applications Conference*, 64 – 73. 1992.

*B. Berliner, "Large risks and limits of insurability," *The Geneva Papers on Risk and Insurance*, 10(37):313–329, October 1985.

R. S. Betterley, *Cyber/privacy insurance market survey*, 2016.

*R. S. Betterley, *Understanding the cyber risk insurance and remediation services marketplace*, 2010.

*C. Biener, M. Eling, and J. Wirfs, *Insurability of cyber risk: an empirical analysis*, Institute of Insurance Economics, 2015.

*S. Bistarelli, M. Dall'Aglio, and P. Peretti, "Strategic games on defense trees," *Proceedings of 4th International Workshop on Formal Aspects in Security and Trust*, 1–15, 2007.

*R. B¨ohme, *Cyber-insurance revisited*, *Proceedings of the 4-th workshop on the Economics of Information Security*, June 2005.

R. B¨ohme, and G. Kataria, "Models and measures for correlation in cyber insurance," *Proceedings of the 5-th Workshop on Economics of Information Security*, 2006.

*R. B¨ohme and G. Schwartz, "Modeling cyber insurance: Towards a unifying framework", *Proceedings of the 9th Workshop on the Economics in Information Security*, 2010.

*J. Bolot and M. Lelarge, *A new perspective on internet security using insurance*, Technical Report RR-6329, INRIA, 2007.

*J. Bolot and M. Lelarge, "A new perspective on internet security using insurance," *Proceedings of the 27th IEEE International Conference on Computer Communications*, 1948–1956, 2008.

*J. Bolot and M. Lelarge, *Managing Information Risk and the Economics of Security*, chapter Cyber Insurance as an Incentive for Internet Security, 269–290, 2009.

*J. Bradford, *Network security & cyber risk management: The fourth annual survey of enterprise-wide cyber risk management practices in Europe*, Advisen Ltd., February 2015.

J. R. Busemeyer, and J. T. Townsend, "Decision Field Theory: A dynamic cognition approach to decision making," *Psychological Review*, 100, 432–459, 1993

*S. A. Butler, "Security attribute evaluation method: a cost-benefit approach, *Proceedings of the 24th International Conference on Software Engineering (ICSE'02)*, 232–240, ACM Press, 2002.

*S. A. Butler, *Security attribute evaluation method*, Technical Report CMU-CS-03-132, Carnegie Mellon University, May 2003.

C. Camerer, *Prospect Theory in the Wild: Evidence from the Field*, In Choices, Values and Frames, edited by Daniel Kahneman and Amos Tversky, Cambridge University Press, 2000.

C. Camerer and H. Kunreuther, "Experimental Markets for Insurance," *Journal of Risk and Uncertainty*, 2, 265-300, 1989.

C. Camerer, and M. Webber, "Recent Developments in Modeling Preferences: Uncertainty and Ambiguity," *Journal of Risk and Uncertainty*, 5:325-370, 1992.

*R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, *Improving the information security risks assessment process*, Technical Report CMU/SEI-2007-TR-012, Software Engineering Institute, May 2007.

*E. Chabrow, *10 concerns when buying cyber insurance*, BankInfoSecurity, June 2012.

*M. E. Christian Biener and J. H. Wirfs, "Insurability of cyber risk", *Newsletter on Insurance and Finance*, (14), 2014.

*M. Crane, "International liability in cyberspace," *Duke Law & Technology Review*, 1(1):23, 2001.

G. Dionne, and S. Harrington. *An Introduction to Insurance Economics*, In G. Dionne and S. Harrington (eds.), Foundations of Insurance Economics, Kluwer Academic Publishers, 1992.

H. J. Einhorn, and R. M. Hogarth, "Ambiguity and Uncertainty in Probabilistic Inference", *Psychological Review*, 92 (4), 433-464, 1985.

R. Eisner and R. H. Strotz, "Flight Insurance and the Theory of Choice," *Journal of Political Economy*, 69, 355-368, 1961.

D. Ellsberg, “Risk, ambiguity, and the Savage axioms”, *Quarterly Journal of Economics*, 75, 643-669, 1961.

*ENISA, *Incentives and barriers of the cyber insurance market in Europe,* ENISA, June 2012.

*ENISA, *Introduction to Return on Security Investment*, ENISA, December 2012.

C. R. Fox, and K. E. See, *Belief and preference in decision under uncertainty*. Chapter in D. Hardman and L. Macchi (Eds.), Thinking: Current Perspectives on Reasoning, Judgment, and Decision Making, 2003.

FSSCC, *Cyber Insurance Buying Guide*, Financial Services Sector Coordinating Council, 2016.

*R. Fredriksen, M. Kristiansenand, B. A. G. K. Stølen, T. A. Opperud, and T. Dimitrakos, “The CORAS framework for a model-based risk management process”, *Proceedings of the 21st International Conference on Computer Safety, Reliability and Security*, volume 2434 of Lecture Notes in Computer Science, 94–105, 2002.

*J. Freund and J. Jones, *Measuring and Managing Information Risk A FAIR Approach*, Elsevier, 2015.

*D. Geer, “Risk management is still where the money is”, *Computer*, 36(12):129–131, 2003.

D. Geer , K.S. Hoo, A. Jaquith, “Information Security: Why the Future Belongs to the Quants”, IEEE Security and Privacy, 1(4), 32-40, 2003.

M. T. Glascott, and A. J. Aisen, “The Emperor's New Clothes and Cyber Insurance,” FDCC Quarterly, 200-225, 2013.

*N. Gohring, *Cyber insurance may cover damage of computer woes*, The Seattle Times, July 2002.

*L. A. Gordon and M. P. Loeb, “Managing Cybersecurity Resources: a Cost-Benefit Analysis”, McGraw Hill, 2006.

*L. A. Gordon, M. P. Loeb, and T. Sohail “A framework for using insurance for cyber-risk managemen, *Communication of the ACM*, 46(3):81–85, Mar. 2003.

*B. A. Gran, R. Fredriksen, and A. P.-J. Thunem, “An approach for model- based risk assessment,” *SAFECOMP*, 311–324, 2004.

*M. Greisiger, *Cyber liability & data breach insurance claims*. NetDiligence, 2013.

J. Grossklags, N. Christin, and J. Chuang, “Secure or Insure? A Game-Theoretic Analysis of Information Security Games,” WWW 2008, 209-218, 2008.

*H. S. B. Herath and T. C. Herath. Cyber-insurance: Copula pricing framework and implication for risk management, *Workshop on the Economics of Information Security*, 2007.

J. Hershey, H. Kunreuther, and P. Schoemaker, "Sources of Bias in Assessment Procedures for Utility Functions," *Management Science*, 28, 936-954, 1982.

J. Hershey, and J. H. Shoemaker, "Risk Taking and Problem Context in the Domain of Losses: An Expected Utility Analysis," *Journal of Risk Insurance*, 47(1), 111-132, 1980.

*D. S. Herrmann, Complete Guide to Security and Privacy Metrics, "Measuring Regulatory Compliance", *Operational Resilience, and ROI*, 2007.

*D. Hubbard, and D. Evans, "Problems with scoring methods and ordinal scales in risk assessment," *IBM Journal of Research and Development*, 54(3), May-June 2010.

*C. C. Hsu and B. A. Sandford, "The delphi technique: Making sense of consensus" *Practical Assessment Research & Evaluation*, 12(10), 2007.

*IEC, *IEC 60300-3-9 Dependability management- Part 3. Application guide- Section 9: Risk analysis of technological systems - Event Tree Analysis (ETA)*, IEC, 1995.

*IEC, *IEC 61025:2006. Fault tree analysis (FTA)*, 2006.

Intel, The Cybersecurity Framework in Action: An Intel Use Case, Intel, 2015.

*ISO/IEC, Iso/iec 27018:2014 - information technology – security techniques – code of practice for protection of personally identifiable information (pii) in public clouds, ISO, 2014

*ISO/IEC, *ISO/IEC 27002:2005 Information technology – Security techniques – Code of Practice for Information Security Management*, ISO, 2005.

*ISO/IEC, ISO/IEC 27001: *Information technology Security techniques Information security management systems Requirements*, ISO, 2013.

*A. Jaquith, *Security metrics: replacing fear, uncertainty, and doubt*, Addison-Wesley, 2007.

E. J. Johnson, J. Hershey, J. Meszaros, and H. Kunreuther, "Framing, Probability Distortions, and Insurance Decisions," *Journal of Risk and Uncertainty*, 7, 35-51, 1993.

*S. Jones, "Lloyds CEO Sees Cyber Insurance to Surge After Attacks," *Bloomberg Business*, October 2014.

*B. Karabacak and I. Sogukpinar, "*ISRAM: information security risk analysis method* ", *Computers & Security*, 24(2):147–159, 2005.

H. Kunreuther, R. Hogarth, and J. Meszaros, "Insurer Ambiguity and Market Failure," *Journal of Risk and Uncertainty*, 7 (1), 71-87, 1993.

*J. P. Kesan, R. P. Majuca, and W. J. Yurcik, *The economic case for cybersinsurance*. Technical Report LE04-004, Illinois Law and Economics, 2004.

*L. Krautsevich, F. Martinelli, and A. Yautsiukhin, "Formal approach to security metrics. what does "more secure" mean for you?" *Proceedings of the 1st International Workshop on Measurability of Security in Software Architectures*, ACM Press, 2010.

*L. Krautsevich, F. Martinelli, and A. Yautsiukhin, "Formal analysis of security metrics and risk," *Proceedings of the IFIP Workshop on In- formation Security Theory and Practice, volume 6633 of Lecture Notes in Computer Science*, 304–319, 2011.

*L. Krautsevich, F. Martinelli, and A. Yautsiukhin, "Towards modelling adaptive attacker's behavior," *Proceedings of 5th International Symposium on Foundations & Practice of Security, volume 7743 of Lecture Notes on Computer Science*, 357–364, 2012.

H. Kunreuther, R. Ginsberg, L. Miller, P. Sagi, P. Slovic, B. Borkin, and N. Katz, *Disaster Insurance Protection: Public Policy Lessons*, Wiley, 1978.

*Y. Leanid Krautsevich, and F. Martinelli, "Formal analysis of security metrics with defensive actions, *The 10th IEEE International Conference on Autonomic and Trusted Computing*, 2013.

*M. Lelarge and J. Bolot, "Network externalities and the deployment of security features and protocols in the internet" *SIGMETRICS Perform. Eval. Rev.*, 36(1):37–48, June 2008.

*M. Lelarge and J. Bolot, "Economic incentives to increase security in the internet: The case for insurance," *In Proceedings of the 28th IEEE International Conference on Computer Communications*, 1494–1502, 2009.

*M. S. Lund, B. Solhaug, and K. Stolen, *Model-Driven Risk Analysis*, Springer, 2011.

*P. Luzwick, "If most of your revenue is from e-commerce, then cyber- insurance makes sense," *Computer Fraud & Security*, 3:16–17, March 2001.

*F. Martinelli, and A. Yautsiukhin, "Security by Insurance for Services", *IEEE International Conference on Software Quality, Reliability and Security Companion*, 2016.

*S. Mauw and M. Oostdijk, *Foundations of attack trees. In Proceedings of the 8th International Conference on Information Security and Cryptology, Lecture Notes in Computer Science*, Springer-Verlag, 2005.

*R. Mehr and E. Cammack, *Principles of insurance. Richard D. Irwin, inc., third edition* 1961.

*T. Mikosch, *Non-life insurance Mathematics*, Springer, 2009.

T. Moore, "The economics of cybersecurity: Principles and policy options," *International Journal of Critical Infrastructure Protection*, 3(3–4):103 – 117, 2010.

*A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, and S. K. Sad- hukhan, "Cyber-risk decision models: To insure it or not?" *Decision Support Systems*, 56:11–26, 2013.

*G. K. Mukhopadhyay, Shukla, P. Kirs, and K. K. Bagchi, "Quantifying e-risk for cyber-insurance using logit and probit models, *Proceedings of the 8th Annual Symposium on Information Assurance*, 2013.

*P. Naghizadeh and M. Liu, "Voluntary participation in cyber-insurance markets", *Proceedings of the 2014 Annual Workshop on Economics in Information Security*, 2014.

NAIC, *Cybersecurity*, National Association of Insurance Commissioners, 2015.

NIST, *Framework for Cyber-Physical Systems*, release 1.0, Cyber Physical Systems Public Working Group, May 2016.

NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, 2014.

*NIST, *Guide for conducting risk assessment*, Technical Report SP 800-30 Revision 1, National Institute of Standards and Technology, September 2012.

*S. Noel and S. Jajodia, "Managing attack graph complexity through visual hierarchical aggregation", *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, 109–118, 2004.

NPPD, *Cyber Incident Data and Analysis Working Group, Enhancing Resilience Through Cyber Incident Data Sharing and Analysis*, National Protection and Programs Directorate, 2015.

NPPD, *Cyber Security Insurance Workshop Readout Report*, National Protection and Programs Directorate U.S. Department of Homeland Security, 2014.

NPPD, *Cyber Risk Culture Roundtable Readout Report*, National Protection and Programs Directorate U.S. Department of Homeland Security, 2013.

NPPD, *Cyber Security Insurance Workshop Readout Report*, National Protection and Programs Directorate U.S. Department of Homeland Security, 2012.

*H. Ogut, N. Menon, and S. Raghunathan, "Cyber insurance and it security investment: Impact of interdependent risk," *Proceedings of the 4-th Workshop on the Economics of Information Security*, 2005.

*R. Ortalo, Y. Deswarte, and M. Kaaniche, "Experimenting with quantitative evaluation tools for monitoring operational security," *IEEE Transactions on Software Engineering*, 25(5):633–650, 1999.

*R. Pal, "Cyber-insurance for cyber-security: a solution to the information asymmetry problem", *Proceedings of SIAM Annual Meeting*, 2012.

*R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? a market analysis," Proceedings of the 2014 INFOCOM, 235–243, 2014.

R. Pal, and P. Hui, "On Differentiating Cyber-Insurance Contracts a Topological Perspective," *Internet Management Conference*, 2013.

*J. H. Pardue and P. Patidar, "Threats to healthcare data: a threat tree for risk assessment," *Issues in Information Systems*, XII(1):106–113, 2011.

Ponemon Institute, *2015 Global Cyber Impact Report*, AON-Ponemon Institute, 2015

Ponemon, *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*, Ponemon Institute, 2013.

*PWC, *Managing cyber risks in an interconnected world*, PWC, 2014.

*S. Radosavac, J. Kempf, and U. C. Kozat, "Using insurance to increase internet security," In J. Feigenbaum and Y. R. Yang, editors, NetEcon, pages 43–48, 2008.

*K. Saini, I. Azad, N. B. Raut, and L. A. Hadimani, "Utility implementation for cyber risk insurance modeling," *Proceedings of the World Congress on Engineering*, 2011.

*F. B. Schneider, "Enforceable security policies," *ACM Transactions on Information and System Security*, 3(1):30–50, 2000.

B. Schneier *The Psychology of Security*, 2008.

*B. Schneier, "Attack trees: Modelling security threats," *Dr. Dobb's journal*, December 1999.

D. Schutzer, "An Assessment of Cyber Insurance," *CTO Corner*, 2015.

*N. Schwartz, N. Shetty, and J. Walrand. Cyber-insurance: Missing market driven by user heterogeneity, Workshop on the Economics of Information Security, 2010.

*Schwartz, N. Shetty, and J. C. Walrand, "Why cyber insurance contracts fail to reflect cyber risks," *Proceedings of the 51st annual Allerton Conference*, 781–787, 2013.

*A. Schwartz and S. S. Sastry, “Cyber-insurance framework for large scale interdependent networks,” *Proceedings of the 3rd International Conference on High Confidence Networked Systems*,” 145–154, 2014.

SEC, “CF Disclosure Guidance: Topic No. 2,” 2011.

*S. J. Shackelford, “Should your firm invest in cyber risk insurance?” *Business Horizons*, 55(4):349 – 356, 2012.

*N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand, “*Economics of Information Security and Privacy*, chapter Competitive Cyber-Insurance and Internet Security, 229–247, 2010.

*O. Sheyner and J. Wing, “Tools for generating and analyzing attack graphs,” *Proceedings of Formal Methods for Components and Objects, Lecture Notes in Computer Science*, 2005.

*W. Shim, “An analysis of information security management strategies in the presence of interdependent security risk,” *Asia Pacific Journal of Information Systems*, 22(1), March 2012.

*G. Stoneburner, A. Goguen, and A. Feringa, *Risk management guide for information technology systems*, Technical Report 800- 30, National Institute of Standards and Technology, 2001.

J. Sydnor, "(Over)insuring Modest Risks," *American Economic Journal*: Applied Economics, 2(4): 177-99, 2010.

A. Tversky, and D. Kahneman, “Advances in prospect theory: Cumulative representation of uncertainty,” *Journal of Risk and Uncertainty*, 5(4), 297-323, 1992.

*The IT Governance Institute. Cobit 4.1.

*J. Vaughan and T. M. Vaughan, *Fundamentals of Risk and Insurance*. Wiley, 11th edition, 2014.

*D. Verdon and G. McGraw, “Risk analysis in software design,” *IEEE Security and Privacy*, 2(4):79–84, 2004.

*R. von Solms, and J. V. Niekerk, “From information security to cyber security,” *Computers & Security*, 38:97–102, 2013.

*Z. Yang and J. C. S. Lui, “Security adoption and influence of cyber insurance markets in heterogeneous networks,” *Performance Evaluation*, 74:1–17, 2014.

J. Volkman-Wise, “Representativeness and managing catastrophe risk,” *Journal of Risk and Uncertainty*, 51:267–290, 2015.

*W. Yurcik and D. Doss, “Cyberinsurance: A market solution to the internet security market failure, In Proceedings of the 1-st Workshop on the Economics of Information Security, 2002.

*X. Zhao, L. Xue, and A. B. Whinston, “Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling,” *Proceedings of the International Conference on In- formation Systems, ICIS*, 2009.

S. Yu, Cyber Defense Matrix “Understanding the Security Vendor Landscape Using the Cyber Defense Matrix,” *RSA Conference*, 2016