**Journal of Information Security, 2016, 7, 15-28**
Published Online March 2016 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2016.72002

Scientific Research Publishing

# Cybersecurity Investment Guidance: Extensions of the Gordon and Loeb Model

**Scott Farrow[1], Jules Szanton[2]**

[1]Department of Economics, UMBC, Baltimore, USA
[2]Center for Health and Homeland Security, University of Maryland, Baltimore, USA
Email: farrow@umbc.edu, jules.szanton@umaryland.edu

Received 10 November 2015; accepted 13 March 2016; published 16 March 2016



## Abstract

**Extensions of the Gordon-Loeb [1] and the Gordon-Loeb-Lucyshyn-Zhou [2] models are presented based on mathematical equivalency with a generalized homeland security model. The extensions include limitations on changes in the probability of attack, simultaneous effects on probability and loss, diversion of attack, and shared non-information defenses. Legal cases are then investigated to assess approximate magnitudes of external effects and the extent they are internalized by the legal system.**

## Keywords

**Cybersecurity, Investment, Externality, Log-Convexity, Law**

## 1. Introduction

The most pressing cyberthreats once came from emailed viruses, but today's cyberattacks increasingly take the form of massive identity and intellectual property thefts and the potential for physical damage to critical infrastructure. As cyberattacks have proven to be increasingly disruptive to the economy, a growing body of scholarship examines how much firms should invest in protection and what are appropriate roles for governments. Gordon and Loeb, GL [1], and later, Gordon, Loeb, Lucyshyn and Zhou, GLLZ [2], are leaders in examining the optimal level of spending that organizations should optimally invest in cybersecurity. Their approach uses an unconstrained expected profit maximization model where cybersecurity investments are separable from other activities of the firm. The benefit to the firm from a cybersecurity investment is a cost reduction; the remaining probability of a security breach (S(z)) times the loss (L), which can be altered based on investing in cybersecurity, z. GL analyzed direct (private) damages while GLLZ extended the model to include external damages.

GL and GLLZ investigate the implications of their model in some detail after first deriving the condition that

**How to cite this paper:** Farrow, S. and Szanton, J. (2016) Cybersecurity Investment Guidance: Extensions of the Gordon and Loeb Model. *Journal of Information Security*, **7**, 15-28. http://dx.doi.org/10.4236/jis.2016.72002

the optimum (interior) investment is found where the incremental benefits of information security equal the incremental costs. As the optimal investment is shown to be increasing in damages (losses), including external damages increases the optimal level of investment. As with standard models of investment, an organization that only considers private losses in its optimization is correct if there are no external losses; but if external losses exist then optimum social expenditures increase. By investigating several functional forms for the security breach function, GL and later researchers showed that it is not uncommon for investments to have a maximum of about 37 percent of expected losses although this result is conditional on the specification.

This paper proceeds by investigating extensions to the GL and GLLZ models implied by a general investment model for homeland security expenditures. A review of legal cases involving cybersecurity breaches is then used to assess the implications of including external costs in the optimal investment model.

## 2. Extensions of the GL and GLLZ Models Using a Homeland Security Model

While GL and GLLZ examine how much an individual firm should invest in preventing a cyberattack, related work by Farrow [3] investigates a set of expected, constrained cost minimization models for homeland security expenditures. The models were originally conceived to support Government performance audits in the US Government Accountability Office. The GL, GLLZ and Farrow models make similar simplifying assumptions about the relevance of expected value decision-making, continuity and derivatives of key functions[1]. The core similarities and differences are investigated below followed by several extensions presented in Farrow. The extensions illustrate modifications to investment rules where there are different types of constraints, interactions, and investment alternatives.

A summary of the definitions for the general homeland security investment model based on Farrow [3] is below. The "organization" referred to was originally modeled as the government, since governments are expected to consider both direct and external effects and assumed to select the socially optimal outcome. The organization could also be a firm or consumer. However, these organizations are typically modeled as having different objective functions. While the government is concerned with minimizing overall social costs, a self-interested firm or consumer will not consider the external effects of its choices unless there is some feedback mechanism, such as legal liability, which incentivizes the firm or individual to internalize the costs it creates for others.

Define:

$e_i$: organizational security expenditures on site $i$.

$\bar{E}$ : an aggregate expenditure constraint over all sites and pathways.

$P(e_i)$: probability of an event. $P' < 0$; $P'' > 0$ where $P'$ is the partial derivative and functions are assumed to be twice continuously differentiable. This assumes some behavior or reaction function on the part of the attacker such that expenditures could alter their choice of targets or the expenditures could lead to capture prior to an attack.

$S(e_i)$: additional costs incurred as a result of the investment expenditure whether for the expending organization or third parties such as time in security lines or changes in productivity which are not part of the budget constraint, expect $S' > 0$.

$C(e_i)$: social cost given an event happens, $C' < 0$; $C'' > 0$, which includes direct costs to the organization, $C^D(e_i)$ and costs external to the organization (external costs) $C^E(e_i)$. Note that the constrained expenditure amount $e_i$ is always assumed to be obligated and spent whether or not an attack occurs. It is the social cost, $C$, that is conditional on the event occurring.

The organization's investment problem is stated as choosing the level of expenditure at each site ( $e_i^* \geq 0$ ) in order to minimize expected social cost:

Min

$$\sum_{i=1}^{N} P(e_i)\left[C(e_i)+e_i+S(e_i)\right]+\left[1-P(e_i)\right]\left(e_i+S(e_i)\right)$$

Subject to:

[1]Hausken [4] investigates some of the assumptions noting how the skills of the attackers may affect the convexity (leading to an interior solution), or the concavity (leading to a corner solution) of the problem. Game theoretic concerns about the assumptions may be somewhat abated by noting that the initial probability of a breach is not constant across sites but reflects the interests of the attacker, and that the change, if any, in probability of a security breach empirically reflects the behavioral response of the attacker.

$$\sum_{i=1}^{N} e_i = \bar{E}$$

$$e_i \geq 0$$

The unconstrained minimization form of the problem is that used by Baryshnikov [5] in his extension of the underlying mathematical properties of the GL model and by Gordon, Loeb and Lucyshyn [6]. The GL and GLLZ models can be seen as the dual of the Farrow model prior to the inclusion of constraints—maximizing cost reductions is the dual of minimizing costs for an interior solution [6].

GL and GLLZ do not consider a budget constraint, although they note that conflict between the Chief Information Officer and the Chief Executive Officer may affect the derivation of the optimal amount. In many instances, a budget constraint may be a more realistic decision context. In the budget constrained problem, a budget larger than the optimum expenditure yields the unconstrained solution (the constraint is not binding) while a binding constraint implies a shadow price affecting the expenditure allocation. At the same time, the parameterization in GL adds greater interpretation to the Farrow results.

The notation changes and constraints to place the GL model in the Farrow notation are as below (**Table 1**).

Farrow investigated several cases which can be considered extensions of the GL and GLLZ models[2]. Security and investment concerns modeled by these extensions include:

1) Multiple sites with a budget constraint: The primary difference compared to GL and GLLZ is inclusion of the shadow price of the constraint. First order conditions require that the marginal (incremental) benefit of the investment equal the marginal cost at each site where the marginal cost takes into account the shadow price associated with the binding constraint. Further, marginal expected social costs avoided—the benefits—are to be equated across sites. Where such equality cannot occur, some sites have zero optimal investment. In application, GL appear to follow such an approach for multiple information sets [7].

2) Probability and consequence reductions: Investments may reduce not only the probability of an attack but the loss from the attack. When these impacts are separated, investments should occur until the incremental return per dollar invested is the same across the probability and consequence domains. Recent cybersecurity approaches echo this conclusion by extending cybersecurity beyond protecting access to actions designed to limit internal and external damage.

3) Attacker diversion: Investments in defense by one organization may divert attacker effort to another site. If larger firms are better protected than smaller firms, whether in the defense industry or elsewhere; the probability of attack may increase at less defended sites.

4) Continuous asymmetric focus or advanced persistent attack: Limitations on ability to defend a site or consequences of an attack may lead to optimal *inequality* of defense across sites and information sets as security may not be reducible to the level desired in the absence of such persistent attacks.

5) Shared filtering or defenses: The benefit of the investment includes the sum of benefits across all units to the extent that defensive activity reduces damages at other sites through positive external effects. This may occur for example if government or the private sector provides centralized hacker detection. The centralization

**Table 1.** Notation changes and equivalencies.

| Underlying concept | GL original notation | Farrow notation | Note |
|---|---|---|---|
| Sites or information set; unit of analysis | One unit | Multiple sites $i$ | $i = 1$ for equivalence |
| Investment (expenditure) in cybersecurity | $Z$ | $e$ | Equivalent |
| Probability of successful attack given an investment level | $S(z)$<br>Security breach function | $P(e)$<br>Terrorism event function | Equivalent (but modified initial limits of prob. not incorporated in Farrow) |
| Conditional cost or loss of an event | $L$<br>Initially, $L$; later $L^P + L^E$ for private and external | $C(e)$<br>Includes both direct and external, $C^P$ and $C^E$<br>$C = L^P + L^E$ | GL is constant<br>GL start with $L^P$, Farrow starts with $C = C^P + C^E = L^P + L^E$ and as a function of expenditures |

[2]See [3] for the formal model statements, derivations and further discussion.

may protect a number of sites and returns to scale may exist such that there is a low marginal cost to protect more users. (Note that the potential for external public bads of a security breach are included in the social cost of the base model). Game theoretic models for firm decision-making with free-riding or probability of a breach elsewhere in the network typically lead an individual firm to underinvest in shared information or individual defenses [6] [8].

6) All hazards and/or false negative and false positive outcomes: As with most applications of uncertainty, there is often a chance of incorrectly applying a defensive method; or of failing to apply a defensive method. For instance, as cybersecurity defense may move from "signature" identification of problematic sites or malware toward "behavioral" identification based on the actions of software; it may be that the probability of a "false positive" increases. A false positive in this case is when an action is indeed appropriate, but the behaviorally based software identifies the action as inappropriate. There is a cost associated with such false positives, even if the focus is often on the costs of the false negatives-those actions that are indeed "bad" but are not identified as being bad. The investment model extends naturally to include the additional probabilities and costs associated with this broader set of actions. A similar concern may occur if a cyber expenditure reduces the hazard of a cyber-physical system breach but increases the probability of a false (positive) signal to the cyber-physical system.

These extensions of the cybersecurity model and their resulting optimum conditions are summarized below (**Table 2**).

## 3. Maximum Cybersecurity Investments

Expected value optimization models generally bound investments to lie between zero and the expected value of losses based on the boundary conditions of the problem. An important analysis in GL was the additional step of considering specific functional forms for the security breach function, S. Their rather dramatic conclusion was that for the forms investigated, the optimal security investments would not exceed about 37 percent (1/*e*) of the initial expected loss. This conclusion has been the subject of additional research by Willemson [9], Hausken [4] and Baryshnikov [5] indicating that while a significant class of functional forms (log convex with independent security effects of additional investments) follows the 1/*e* limit; other forms, such as linear, extend the full range of possible investment up to the value of the expected loss.

Recent work on log convexity and log concavity by Bagnoli and Bergstrom [10] informs the sensitivity of log convexity to functional form. Starting with S, the security breach probability in GL and GLLZ; it represents the remaining probability of a breach (or break) after an investment z. A statistical interpretation is that it represents a reliability function (or exceedance function), the complement of a cumulative distribution function. The initial probability of a breach, v, would then be the initial reliability which can range between zero and one. The difference between v and S is the increase in reliability or conversely the decrease in the probability of a breach. Bagnoli and Bergstrom [10] investigate the log-concavity and convexity of numerous reliability functions (after investigating the implications of various transformations). They catalog a large number of common probability

**Table 2.** Optimality conditions for extensions of the GL model.

| Issue/model | Summary of Socially Optimum Condition |
|---|---|
| Allocating a Total Defensive Expenditure among Multiple Independent Sites. | Equate the marginal expected social costs avoided (MESCA) across sites; possibly no protection at some sites. |
| Advanced Persistent Threat: Technological or Behavioral Constraint on Probability or Cost Reduction. | Technological or behavioral constraints can result in an optimal inequality among sites even where investment occurs. |
| Allocation of Expenditures Across Damage and Probability-Reducing Activities. | Equate the marginal social cost avoided of each type of expenditure where expenditures are positive (some may be below threshold). |
| Public Goods, Border control and Positive Interdependencies. | Invest until the sum of their marginal damage cost avoided equals the individual site MESCA. |
| Site Interdependencies Due to Displacing the Probability of Attack. | Determine the net MESCA, net of probability increasing effects at other sites; sites of attack may be spread but social costs reduced. |
| Multiple Sources of Probability (All Hazards) and Cost, as with false positives and false negatives from behavioral controls. | The form of the allocation decision is the same (e.g. equate MESCA), but all costs and probabilities should be taken into account. |

and cumulative density, and reliability functions. Log-concavity appears to dominate but some distributions are log-convex in their density functions and log-concave in other functions. The conclusion drawn by this author is that the functional form of the security breach function is an empirical question with numerous candidate forms implying the range of loss, in the expected value model, is from zero to the expected loss. This is consistent with the discussion in GL and GLLZ, that specification matters. Quantification of any expenditure bounds in the Farrow model are expected to follow those of the GL model given the equivalent mathematical structure.

## 4. External Effects: A Legal Analysis

Optimal security expenditures increase as expected damages increase [1]. Because GLLZ include external damages in their calculation of expected damages, they find that the socially optimal expenditure on cybersecurity increases without bound as external damages increases. However, the $1/e$ (~37%) rule applies to the external losses as well as private losses with a log-convex specification with independent security effects[3]. While optimal investment with externalities may be unbounded, GLLZ established a reference point by analyzing "How large must external losses be as a proportion of private losses in order for optimal investment to equal expected private losses?" Through a numerical example they establish that an external loss that is 180% of private losses would imply an optimal investment approximately equal to the expected private loss of the firm. The exact reference proportion (and percent if multiplied by 100) is a constant that can be derived from the GLLZ model as $e - 1$, or ~1.718 (172%). GLLZ call an external loss exceeding the reference point of ~180% of expected private losses as being "extremely large", implying that a firm may often be acting in society's best interest when it spends less on cybersecurity than its expected private cost.

A legal approach is taken here to inform the empirical magnitude of external losses. The investigation focuses on the magnitude and extent to which an attacked firm is liable for damages to additional parties, the external costs. Although the attacked firm is itself a victim, the incentives the firm faces to undertake defensive actions reflects in part the losses it may incur through legal action (or through insurance payments reflecting the potential for legal action).

A close look at several data breaches shows that an external cost of more than 180% of the private cost is not unusually large for some types of attacks indicating optimal social expenditures in excess of private expected losses[4]. While larger expenditures are consistent with GLLZ, this finding indicates that the reference point of expected private losses may not be particularly relevant. Firms face risks of many different sorts of data breaches. Some data breaches target consumers' financial information, others target a firm's intellectual property, while other breaches target connections between cyber and physical infrastructure. Each type and incidence of breach may have different private and external costs. Yet in many of the cases discussed below, external costs are much larger than private costs, and the legal system is unable to assign legal liability to data-storing firms in a manner that effectively internalizes the external costs of a data breach.

### 4.1. Personal Identity Theft

Personal identity (PI) theft is one of the more visible breaches of cybersecurity when attackers gain personal information from human resource departments, stored billing information or other databases. In PI cases, the perpetrator of a data breach generally seeks information about third-parties (e.g. customers), not information about the company whose servers are breached. Not surprisingly, these data breaches have the potential to create high levels of external costs.

When there are external costs of a personal information data breach, third-parties who lose money (including customers, their financial institutions, and their credit card companies) often sue the directly attacked firm. These plaintiffs have enjoyed varying degrees of success in the legal system. In some cases, plaintiffs have recovered a portion of their costs from legal settlements. When a plaintiff receives a settlement from the directly attacked firm, the external cost from the data breach is reduced and the private cost as defined by GL increases.

[3]For purposes of this section, the "private cost" of a data breach is the cost incurred by the directly attacked firm, and the "external cost" of a data breach is the cost incurred by the rest of society. This conception of "external cost" is narrower than the definition employed by Cohen [11] in the crime literature, who defines the "external cost" of a crime as "a cost imposed by one person onto another, where the latter person does not voluntarily accept the negative consequence." For the purpose of this section, however, the "external cost" excludes the cost to the directly-attacked firm.

[4]Several cases were selected as being large and identifiable, others as setting important legal precedents, and others chosen at random from the data breach data base at the Privacy Rights Clearinghouse (www.privacyrights.org/).

In other cases, plaintiffs were not able to recover because they were unable to show standing, were prevented from recovering due to the economic loss doctrine, or faced some other legal or practical barrier to recovery. In these cases, the plaintiffs' external costs remain external costs and are not expected to enter the private benefit-cost calculation as discussed by GLLZ.

The Heartland Payment Systems data breach is an example of third parties recovering some of the external costs of a data breach, but still losing more the reference point of 180% of the private cost. Heartland Payment Systems is a major payment processing company [12]. In 2007, malware was implanted in Heartland's servers leading to the theft of 130 million customers' credit card. Heartland faced five lawsuits from third parties: a class-action suit from consumers; suits from Visa, MasterCard, and American Express, each of which filed the suits together with affiliated card-issuing financial institutions; and a suit from financial institutions that sued independently from the credit card companies.

In settling four of the suits, Heartland partially internalized the external costs that the breach had imposed on financial institutions and consumers. Heartland paid a total of $105 million to VISA, MasterCard, American Express, and financial institutions that issued credit and debit cards through these companies. This appears to be far less than the full damages suffered by the plaintiffs. As Graves, Acquisti, and Christin [13] showed, between 60% and 90% of compromised credit cards are reissued by financial institutions after a data breach. The same study showed that when second-order costs are considered, an issuer does not save money by not reissuing the cards. Therefore, a data breach costs the card issuer roughly the same amount regardless of whether the issuer reissues the cards or not. Crosman [14] estimated the cost of reissuing credit cards ranges from $2.70 to $11 per card, while the cost of reissuing debit cards ranges from $2.99 to $12.75 per card. The cost depends on the size of the financial institution; large banks can reissue for less than smaller community banks and credit unions. The theft of 130 million records from Heartland, implies that the credit card companies and affiliated financial institutions lost between $350 million (assuming a loss of $2.70/card) and $1.7 billion (assuming $12.75). The $105 million in settlements that the financial institutions received in settlements was a fraction of their external costs. Assuming that the entire settlement went to the financial institutions (in reality, some of it was consumed in legal expenses) the financial institutions' uncompensated losses would be somewhere between $250 million and $1.6 billion.

Consumers also lost money in the Heartland Security breach and filed a class-action suit against Heartland. Heartland settled the suit for $3 million. Under the terms of the settlement, consumers were eligible for up to $175 in compensation if they could show, by a preponderance of the evidence, that they had lost time or money cancelling a credit card or as the result of unauthorized credit cards. Consumers were also eligible for up to $10,000 if they could show that they had suffered identity theft as a result of the breach. Only 11 consumers successfully qualified for relief, and they received a combined total of just $1925. The rest of the $3 million settlement was spent on legal fees, administrative costs, and a *cy pres* payment to a non-profit focused on information security [12]. While the settlement increased Heartland's private costs by $3 million, it only compensated consumers' external costs by $1925. It is difficult to believe that $1925 represents the socially optimal expenditure to avoid external costs for the 130 million consumers.

Heartland has estimated its private cost from the data breach as $140 million, a figure that includes the $108 million in settlements ($105 million to the financial institutions, and $3 million to the consumers), plus legal fees and other expenses [15]. It is challenging to put an exact figure on the external losses, but it is clear that they are greater than $250 million, which would be 180% of Heartland's private costs. As shown above, the external cost to financial institutions—after subtracting the $108 million in legal settlements—is likely between $250 million and $1.6 billion. (Without the $108 million in settlements, the financial institutions would have lost between $350 million and $1.7 billion.) Since the external cost to consumers is not negligible (though hard to value) the combined external cost to consumers and financial institutions appears to be extremely large.

While external costs in the Heartland data breach substantially exceeded private costs, the discrepancy would have been even greater had Heartland's legal settlements not decreased the external costs and increased the private costs. In other major data breaches, courts have thrown out lawsuits against directly attacked firms. In these data breaches, external costs as a percentage of private costs can be even greater than in Heartland.

Third parties who incur costs as the result of a data breach have struggled to show standing (a sufficient legal basis on which to file suit) since the Supreme Court's decision in *Clapper v. Amnesty International* [16]. A requirement for standing in a federal court is that a plaintiff must have suffered an "injury in fact," which is "concrete and particularized" instead of "merely speculative" as in *Lujan v. Defenders of Wildlife* [17]. In *Clapper*,

the Court held that the "injury in fact" must be something that either already happened or is "certainly impending," not something that might happen in the future. Furthermore, a plaintiff cannot "manufacture" standing by "incurr[ing] certain costs as a reasonable reaction to a risk of [future] harm" [16]. In a data breach case, a consumer will often wish to sue before becoming the victim of identity theft. Similarly, a financial institution may wish to reissue credit cards before the credit or debit cards are misused. Under the rule announced in *Clapper*, the legal system may be unable to reimburse third-party data breach victims for these costs likely increasing the external component of losses.

The Zappos data breach [18], which occurred in 2012, is an example of a data breach in which the legal system has done little to turn external costs into private costs. The perpetrators of the breach stole 24 million customers' names, email addresses, billing and shipping addresses, phone numbers, the last four digits of payment card numbers, and encrypted passwords. No credit card numbers were compromised, so financial institutions did not sue. A class-action suit from Zappos consumers alleged that they faced an increased risk of identity theft. In addition to facing an increased risk of identity theft, the consumers asked to be compensated for credit monitoring purchases that they had made. The United States District Court for the District of Nevada cited *Clapper* [16] in dismissing the suit, holding that the consumers did not suffer the sort of injury that could confer standing in federal court. Judge Jones wrote that his court "realizes that [dismissing the suit] is a frustrating result where Plaintiffs' fears of identity theft and fraud are rational, and it recognizes that purchasing monitoring services is a responsible response to a data breach. Nevertheless, costs incurred to prevent future harm is not enough to confer standing, even when such efforts are sensible" [18]. While the consumer litigation was dismissed,[5] Zappos settled a separate lawsuit with nine state attorneys general for $106,000. But aside from this payment, none of the data breach's external costs were converted to private costs and so the external costs are likely to be an extremely large proportion of private costs.

Third parties who suffer external costs in personal information data breaches can also be prevented from recovering by the economic loss rule. In some—but not all—states, the economic loss rule prevents plaintiffs from recovering for negligence when they have only lost money as a result of the alleged negligence. In these states, financial disputes can only be adjudicated through contract law. If a plaintiff cannot show that the defendant breached a contract, then she cannot recover for negligence. The economic loss rule prevented recovery for employees of the University of Pittsburgh Medical Center. These employees were unable to sue their employer for negligence when the hospital lost their personal information when a court found that the employees' only losses had been financial [19].

### 4.2. Intellectual Property Theft

In cases of intellectual property (IP) theft, the relation between external and private losses is likely to be reversed compared to the previous cases: external losses but not private losses are likely to be low at least in the short-term. Some intellectual property data breaches are committed by insiders: employees—often departing ones—who steal records from their employer. These insider breaches of intellectual property are likely to have considerable private costs, although companies that are the victims of these incidents have been fairly successful at using the legal system to reduce those losses. In contrast, American companies impacted by foreign intellectual property attacks—like the Chinese military's Unit 61398—have generally been unsuccessful at using the legal system to reduce their private costs. Yet in either case, there may be little external cost at least in the short-term. For example, when a departing bank employee steals a list of customers who have applied for loans, the customer loses little. In fact, the customer may actually benefit from the data breach. If, for example, the departing employee uses the stolen information to offer the customer a lower interest rate, the external cost of the data breach could actually be a positive benefit to the individual although a private loss to the original firm. In the long run, however, intellectual property theft could create external costs by increasing the cost of information security and decreasing the overall competitiveness of American firms, an external cost to the country.

The 2011 litigation over an intellectual property data breach at Huntington National Bank [20] illustrates the fact that these sort of data breaches can have low (or no) external costs, and private costs that are generally recoverable through litigation. The Huntington breach occurred when employees of Huntington National Bank—loan officers and their administrative assistants—left Huntington for MVB Bank, a rival financial institution which (like Huntington) issued mortgages. Huntington accused the employees of downloading records from 200

[5]The case was dismissed without prejudice, allowing the consumers to submit the suit again if they could show an injury in fact.

loan applications before leaving Huntington for MVB. Huntington alleged that as a result of the ex-employees' conduct, they suffered damage to their reputation and goodwill in the marketplace, lost customers, and lost rights of exclusive possession in their intellectual property. The United States District Court for the Northern District of West Virginia issued a temporary injunction preventing the defendants from using any proprietary information obtained from Huntington National Bank for any business purpose. After the court issued its injunction, the two sides settled. The settlement obligated the ex-employees to refrain from using the proprietary information, to return the documents from Huntington National Bank, and not to contact Huntington customers with whom the ex-employees worked. As stated above, this sort of conduct creates little short-term potential for external costs, since the 200 customers probably would have benefited from MVB offering a more attractive mortgage than the one offered to them by Huntington. This sort of data breach also offers little potential for large private costs, since Huntington obtained a consent decree which prevented MVB from accessing any records the employees might have taken from Huntington, or even contacting any customers the employees worked with at Huntington.

It is harder for American companies that suffer intellectual property data breaches from perpetrators outside the United States to use the legal system to recover their private costs. Westinghouse, an American nuclear power company, suffered several data breaches when hackers from Unit 61398 of China's People's Liberation Army (PLA) broke into the company's network and stole information about the company's strategy for negotiating with a Chinese counterpart [21]. As with the data breach at Huntington National Bank, this theft created almost no short-term external costs. In fact, third-parties might have even benefitted if Westinghouse's Chinese competitors were able to use the stolen information to generate power more inexpensively. The breach likely did create substantial private costs, especially if Westinghouse ended up at a disadvantage in its negotiations with the Chinese firm, or if the company lost market-share to a Chinese competitor with lower costs. A grand jury at the United States District Court for the Western District of Pennsylvania indicted five officers of Unit 61398 for their role in data breaches against Westinghouse and other American firms. This indictment is unlikely to reduce Westinghouse's private costs, since China will almost certainly not extradite the indicted officers. In fact, Westinghouse's private costs could actually increase as a result of its stepping forward and identifying itself as a victim of Unit 61398, since China could retaliate against the company's Chinese interests to punish the company for accusing the PLA unit [21].

Speculation exists that longer term, macroeconomic external effects may occur with large scale intellectual property thefts [22]. A loss of macro-level comparative advantage, for instance in technologically advanced areas, could affect the welfare of the US labor force as well as affecting US based shareholders.

### 4.3. Critical Infrastructure Cyberattacks

A cyberattack that targeted critical infrastructure could create external costs that greatly exceed private costs. The Critical Infrastructures Protection Act [23], a federal law that is part of the USA Patriot Act, defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The Obama Administration has designated 16 sectors of the economy as critical infrastructure.[6]

Like data breaches that target personal information or intellectual property, cyberattacks on critical infrastructure (CI) involve an attacker exercising control over a computer network to which they do not have authorized access or authority. There are, however, important differences between cyberattacks on CI and data breaches that target PI or IP. Perpetrators of PI and IP data breaches primarily attempt to steal information for economic benefit. Perpetrators of CI cyberattacks, on the other hand, are typically motivated by strategic or political goals.

The United States has never experienced a successful, large-scale cyberattack on critical infrastructure, but other countries have. The Russian government is widely believed[7] to have conducted cyberattacks on critical in-

[6]The 16 sectors are: 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.

[7]Russia has never claimed responsibility for the attacks on Georgia, although (as explained below) the cyberattacks appeared to be coordinated with the movements of conventional Russian military forces. A Russian official did, however, eventually confirm the participation of a Russian government-sponsored youth group in the denial-of-service attacks on Estonian websites [24].

frastructure in both Estonia and Georgia. Estonia experienced cyberattacks in 2007 as the Baltic nation was engaged in a dispute with Russia about a monument to Soviet war dead [25]. Many Estonians viewed the monument as a reminder of the Soviet occupation of their country, while Russians viewed the memorial as expressing respect to Soviet soldiers who fell in battle during World War II. On April 26, 2007—one day before the Estonian government was to move the statue from the center of Tallin to a military cemetery—many Estonian websites experienced denial-of-service attacks. The websites of Estonian banks, government agencies, and media outlets were overwhelmed with traffic, causing them to crash. On April 27, the statue was moved as planned, but the attacks continued, reaching their peak on May 9. Desperate to stop the attacks, the Estonian government took the comprehensive action of blocking all internet traffic from outside the country. By May 19, 2007, the attacks ended.

Georgia experienced similar denial-of-service attacks during its war with Russia in the summer of 2008 [26]. Hackers targeted the websites of Georgia's national and local governments, as well as news websites. The National Bank of Georgia's site was also briefly targeted [27]. The cyberattacks appeared to be coordinated with Russia's military operations: the attacks escalated as Russian troops crossed the Georgian border, and targeted websites of specific regions of Georgia as Russia bombed those areas. The cyberattacks were also coordinated with Russia's strategic objections in the war. Just as Russia damaged areas around Georgia's strategic Baku-Ceyhan oil pipeline but did not actually destroy the pipeline, the Russian hackers targeted government and media websites, but declined to target Georgia's electric grid or attack the National Bank's site in a more sustained manner. The impression is that Russia could have done worse damage later if it wanted.

Both of these cyberattacks demonstrated that an attack on critical infrastructure can produce external costs that are significantly higher than the private costs. A leaked American diplomatic cable [28] estimated that Hansabank, the bank whose website was most disabled by the cyberattack, spent €10 million (roughly $14 million, in 2007 dollars) as a result of the attack. €10 million is a suspiciously round number, and reflects the challenge of reaching an accurate estimate. The *New York Times* reported at the end of May 2007 (after the last wave of cyberattacks) that Hansabank had spent $1 million so far fending off the so-called "bots" that were overwhelming its servers [29]. Yet both these estimates only reflect private costs to Hansabank. The bank also lost significant business during the three weeks when its website was either nonoperational or closed off to traffic from outside of Estonia.

Assessing the external cost of the cyberattacks on Estonian banks and other websites is more difficult. Estonia is one of the most technologically sophisticated countries in the world, and by 2007, over 96% of Estonian banking transactions took place online [30]. When Estonian bank websites were either non-operational or closed off to foreign traffic, the Estonian economy was significantly constrained. Yet the damage to the Estonian economy was not catastrophic, and not as bad as it could have been had the cyberattack been marginally more aggressive. The same leaked American diplomatic cable noted that the damage to the Estonian economy could have been significantly worse had the "second wave" of attacks targeted the "poorly-defended" websites of the logistics firms that transport food and gasoline around the country [31]. One indication of the cyberattacks' potential high external cost is the lengths to which the Estonian government has gone to prevent another wave of cyberattacks. Since 2007, Estonia has become a world leader in defending against cyberwarfare, and has played a crucial role in NATO and EU efforts to respond to cyberattacks. In 2008, largely in response to the attacks on Estonia, NATO created a Brussels-based Cyber Defense Management Authority and an Estonia-based Cooperative Cyber Defense Centre of Excellence [32].

Because the cyberattacks against Georgia occurred in the context of a conventional war and were coordinated with war objectives, it is hard to isolate the private and external costs specific to the cyberattack. Hollis [26] explains how the cyberattacks were integrated into Russia's war strategy:

> Russian-oriented hackers/militia took out news and local government web sites specifically in the areas that the Russian military intended to attack in the ground and air domains. The Federal and local Georgian governments, military, and local news agencies were unable to communicate with Georgian citizens that were directly affected by the fighting. ⋯ [The cyberattacks] created panic and confusion in the local populace, further hindering Georgian military response [26].

The cyberattacks didn't just cost Georgia money; they weakened Georgia's ability to fight. The external cost was military, not just financial.

Russia's goal in launching the cyberattacks against Georgia and Estonia was presumably strategic, not eco-

nomic. Russia sought to assert its power throughout the former Soviet Union. To accomplish that goal, Russia did not need to cause massive damage to the economy of Georgia or Estonia; it just needed to demonstrate its capability. Simply by demonstrating the power to disable crucial elements of its rivals' economies, Russia increased its ability to deter its neighbors from defying it. Today, it is likely that when countries in the former Soviet Union (including Estonia and Georgia) consider taking some action that would displease the Kremlin, they consider the possibility that a cyberattack could damage their economy. Some countries may minimize their risk of a Russian cyberattack by making political concessions, or refraining from adopting policies likely to anger Russia. This is an external cost as well.

If the United States experienced a cyberattack on critical infrastructure, the external losses could greatly exceed the private costs. The costs would, of course, depend on what sort of critical infrastructure was attacked. One threat that looms particularly large is the threat of a cyberattack on the electric grid. In 2014, NSA Director Admiral Mike Rogers warned Congress that China and at least one other country had the potential to disrupt large sections of the American power grid. Rogers warned that other countries were already conducting "reconnaissance" to figure out how American electric networks operated, and how they could be shut down online [33]. According to a 2015 report from the University of Cambridge Centre for Risk Studies and the Lloyd's of London insurance market [34], a cyberattack that targeted electricity supply could create huge costs to the American economy. The report models several different attacks. In each one, the external cost of a cyberattack to the economy as a whole greatly exceeds the costs borne by individual electric companies. For example, in a scenario where the U.S. economy loses $1.024 trillion as the result of a catastrophic interruption in the power supply, power companies would only lose $4.21 billion in lost revenue. In a scenario where the economy loses $243 billion, the power companies would only lose $1.15 billion [34]. Because a catastrophic power outage would be extremely disruptive to the economy as a whole, external costs could exceed private costs by two orders of magnitude.

The American legal system may be able to transfer some of the external cost of a critical infrastructure data breach onto the company that suffered the attack. It is difficult, but sometimes possible, to successfully sue a power company for failing to prevent a power outage. In nearly every state of the country, power companies are allowed to limit their liability for an electric outage to cases of "gross negligence," as opposed to the sort of ordinary negligence for which most companies are held liable [35].[7] In New York, for example, a public utility can limit its liability to "gross negligence" or "willful misconduct," and exempt itself from being sued for ordinary negligence [37]. In Maryland, a public utility is allowed to limit its liability to "willful neglect" or "willful default," which is a similar standard [38].

Customers who experience losses as the result of a power outage sometimes are able to show "gross negligence" and recover from electric companies. After the 1977 blackout in New York City, for example, a grocery store successfully recovered from the Con Edison power company when it showed that Con Edison failed to take a number of safety precautions that could have prevented or limited the damage caused by the blackout [37]. Similarly, after Hurricane Sandy, Con Ed reached a settlement with homeowners who lost power in the storm. The power company paid $17 million, and agreed to cancel a $40 million rate increase [39]. It is possible that a third-party victim of a cyberattack on an electric company could sue the electric company, effectively turning the third-party's external costs into the company's private costs. The electricity sector is subject to binding cybersecurity regulation [40]. If an electric company was grossly negligent in failing to meet these cybersecurity standards, it could face liability which would convert its customers' external costs into company private costs.

Despite this thin reed of legal opportunity, third-parties who suffer losses in a critical infrastructure cyberattack are unlikely to recover much of their losses by filing a lawsuit for gross negligence. Occasional successes notwithstanding, it is generally very difficult to show that a public utility was grossly negligent [41]. Furthermore, in a truly catastrophic critical infrastructure cyberattack, an affected company may not have enough money to compensate all the third-party victims. Recognizing that the tort system was a poor means of protecting consumers from cyberattacks, Congress passed the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002 [42]. The SAFETY Act protects companies from liability in the event of a physical or cyberattack, on the condition that the companies employ technology that the Department of Homeland Security finds can be effective at preventing the attack from occurring. Technologies can be certified by the Department of Homeland Security if they comply with the best practices in counterterrorism, and if certified, they are

[8]See for example [36] "Courts are virtually unanimous that provisions limiting a public utility's liability are valid so long as they do not purport to grant immunity or limit liability for gross negligence."

protected from legal liability [42]. The SAFETY Act seems to assume that government and the legal system are better situated to prevent attacks in the first place than to adjudicate liability in the event of an attack.

## 5. Large Losses and Risk Aversion

GL explicitly focused on small losses and used a risk neutral model [1]. Some, although not all, cybersecurity breaches could entail large losses such that private or public decision-makers may be risk averse. For instance, a loss of intellectual property that is the primary asset of a firm, or a breach that endangers a linked cyber-physical system such as the power grid, water, or some transportation modes. In such instances private sector decision-makers are routinely modeled as being risk averse instead of risk neutral. In general, risk aversion implies a willingness to invest to avoid a risky outcome (for instance, a security breach) that exceeds the expected loss in contrast with risk neutrality, as above, where the investment is limited by the expected value [43]. While this result also occurs in the cybersecurity literature, Huang, Hu and Behara [44] demonstrate that the willingness to invest has an upper bound of *conditional* loss even with risk aversion while investments can be less than the expected loss depending on the nature of the asset being threatened, for instance, it if is "irreplaceable" [45].

Economists have considered whether national level, public decision-makers should be risk neutral or risk averse. Influential work by Arrow and Lind presented a model that such decision-makers "should" be risk neutral when, in fact, public decisions are often made where the costs of control appear larger than the expected value implying risk averse decision-making [46]. Stewart, Ellingwood and Mueller [47] have contrasted expected value and risk averse decision-making for the increases in security expenditures since the 9/11 attacks, and in Stewart and Mueller [48] applied that analysis to the Transportation Security Agency. They used a specific functional form for utility and solved for a break-even risk aversion parameter given their estimates of probability. In general, a large degree of risk aversion was necessary to be indifferent between the prior and current security expenditures. In two examples discussed by Stewart, Ellingwood, and Mueller [47], the chosen defensive investment incorporating risk aversion exceeds the expected monetary loss by factors of 2.97 and 125 respectively, noting that with small probabilities the expected loss can be a small fraction of the conditional loss.

The specific point in the context of the GL two outcome model is that expenditures with risk aversion can significantly exceed expected losses in a discrete outcome model.

However, the result for a continuous state model is more ambiguous. While the general point remains that a risk averse decision-maker will expend more than a risk neutral decision-maker, the difference need not be large. In a continuous state setting, damage functions and probability are both varying. If damages are rising faster than the probability is declining, it is possible that no mean value exists. In contrast, for a concave damage function investigated for flooding [49]; the mean values using a risk neutral and a risk averse utility function, and a weighting based on cumulative prospect theory were not substantially different. In part, the large losses where risk aversion can have a significant effect were associated with sufficiently small probabilities that the distinction was small between the mean values using a risk neutral or a risk averse utility function. Like the finding for the security breach function, the importance of risk aversion is an empirical question involving the structural form of damages, probabilities and the utility function.

## 6. Conclusions

GL thoroughly developed an influential model of cyber-security investment with important implications on the size of cybersecurity investment. As with the history of economic modeling, if one is fortunate enough to get clear initial results; then such results often get extended and qualified. Such is the main theme here. The key issues and conclusions identified here are:

- Consideration of externalities is a primary concern for government policy. Although GLLZ imply that externalities are unlikely to be large; evidence from past data breaches and cyberattacks suggests that externalities may be large, and that the legal system often fails to significantly internalize external costs by allocating risks to the original target. Such allocation may or may not be viewed as fair. This conclusion is relatively clear for personal identity theft and infrastructure attacks while the external effect of intellectual property attacks is less well documented in legal findings. These findings can imply significantly larger cybersecurity expenditures than those based solely on internalized, private sector damages.
- While an expected value (risk neutral) decision-maker will not spend more than expected losses and may spend significantly less, the results depend on the empirical functional form for the security breach function.

- When risk neutral investment considerations include: a) multiple datasets or sites, b) public defenses that protect many sites (as opposed to sharing of information), or c) an ability to invest in reducing damages, then the optimal (constrained) level of cyber investment changes and typically requires an optimal security investment based on the equivalency of marginal expected social cost avoided to the extent technologically possible.
- When additional modeling of the (dis)utility of uncertainty is added, whether in the form of irreversible losses or risk aversion; models commonly exist in which investments exceed expected losses.

The overall conclusion drawn here is that while there may be useful rules of thumb for decision-making, those behavioral rules may be incorrect depending on the empirical context of a specific problem including the behavior of attackers. To the extent that government policies and investments tend to focus on cyber issues with larger externalities, make use of public defenses, or be subject to advanced persistent threats, then the socially optimal investment decisions may be larger and differ significantly from those of the private sector.

## Acknowledgements

Appreciation is extended to Larry Gordon, Anupam Joshi, Marty Loeb, Markus Rauschecker, Matt Shabat and an anonymous referee for comments and to Andrew Naviasky for research assistance; to the University of Maryland Center on Health and Homeland Security for coordination of the legal research and to the Department of Homeland Security Cyber Security and Communications division for short term space. Funding was provided by the Department of Homeland Security National Center on the Risk and Economics of Terrorism Events (CREATE).

## References

[1] Gordon, L. and Loeb, M. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, **5**, 438-457. http://dx.doi.org/10.1145/581271.581274

[2] Gordon, L., Loeb, M., Lucyshyn and Zhou, L. (2015) Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, **6**, 4-30. http://dx.doi.org/10.4236/jis.2015.61003

[3] Farrow, S. (2007) The Economics of Homeland Security Expenditures: Foundational Expected Cost-Effectiveness Approaches. *Contemporary Economic Policy*, **25**, 14-26. http://dx.doi.org/10.1111/j.1465-7287.2006.00029.x

[4] Hausken, K. (2006) Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. *Information Systems Frontiers*, **8**, 338-349. http://dx.doi.org/10.1007/s10796-006-9011-6

[5] Baryshnikov, Y. (2012) IT Security Investment and Gordon-Loeb's 1/e Rule. *Proceedings of the* 11*th Workshop on the Economics of Information Security* (*WEIS*), Berlin, 25-26 June 2012.

[6] Gordon, L., Loeb, M. and Lucyshyn, W. (2003) Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, **22**, 461-485. http://dx.doi.org/10.1016/j.jaccpubpol.2003.09.001

[7] Gordon, L. and Loeb, M. (2011) You May Be Fighting the Wrong Security Battles. *Wall Street Journal*, September 26.

[8] Kunreuther, H. and Heal, G. (2003) Interdependent Security. *Journal of Risk and Uncertainty*, **26**, 231-249. http://dx.doi.org/10.1023/A:1024119208153

[9] Willemson, J. (2010) Extending the Gordon and Loeb Model for Information Security Investment. 2010 *International Conference on Availability, Reliability and Security*, Krakow, 15-18 February 2010, 258-261. http://dx.doi.org/10.1109/ARES.2010.37

[10] Bagnoli, M. and Bergstrom, T. (2005) Log-Concave Probability and Its Applications. *Economic Theory*, **26**, 445-469. http://dx.doi.org/10.1007/s00199-004-0514-4

[11] Cohen, M.A. (2000) Measuring the Costs and Benefits of Crime and Justice. In: Duffee, D., Ed., *Measurement and Analysis of Crime and Justice*, Criminal Justice 2000, Vol. 4, National Institute of Justice, Washington DC, 263-316. http://www.ncjrs.org/criminal_justice2000/vol_4/04f.pdf

[12] Heartland Payment Systems, Inc., Customer Data Security Breach Litigation (2012) 851 F. Supp. 2d 1040 (S.D. Tex.).

[13] Graves, J., Acquisti, A. and Christin, N. (2014) Should Payment Card Issuers Reissue Cards in Response to a Data Breach? *WEIS*: *Workshop on the Economics of Information Security*, Pennsylvania State University, State College, 23-24 June 2014. http://www.econinfosec.org/archive/weis2014/papers/GravesAcquistiChristin-WEIS2014.pdf

[14] Crosman, P. (2014) How Much Do Data Breaches Cost? Two Studies Attempt a Tally. *American Banker*.

http://www.americanbanker.com/issues/179_176/how-much-do-data-breaches-cost-two-studies-attempt-a-tally-1069893-1.html

[15] Silver-Greenberg, J. and Schwartz, N. (2012) MasterCard and Visa Investigate Data Breach. *The New York Times*, 31 March 2012. http://www.nytimes.com/2012/03/31/business/mastercard-and-visa-look-into-possible-attack.html?_r=0

[16] Clapper v. Amnesty International (2013) 133 S. Ct. 1138.

[17] Lujan v. Defenders of Wildlife (1992) 504 U.S. 555, 560-61.

[18] Zappos.com, Inc., Customer Data Sec. Breach Litig. (2015). No. 3:12-cv-00325-RCJ-VPC, (D. Nev.).

[19] Willett, B. (2015) Employees Can't Sue Hospital for Negligence, Breach of Contract, After Personal Data Breach. *Reed Smith Technology Law Dispatch*, 12 June 2015.

[20] The Huntington National Bank v. Kokoska, *et al*. (2011) Docket No. 1:11-cv-00063 (N.D. W. Va. Apr 25).

[21] Schmidt, M. and Sanger, D. (2014) 5 in China Army Face U.S. Charges of Cyberattacks. *The New York Times*, 19 May 2014. http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html

[22] Andrijcic, E. and Horowitz, B. (2006) A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property. *Risk Analysis*, **26**, 907-923. http://dx.doi.org/10.1111/j.1539-6924.2006.00787.x

[23] Critical Infrastructures Protection Act (2001) 42 U.S.C. § 5195c(e).

[24] Miller, C. (2009) Russia Confirms Involvement with Estonia DDOS Attacks. *SC Magazine*, 12 March 2009. http://www.scmagazine.com/russia-confirms-involvement-with-estonia-ddos-attacks/article/128737/

[25] Tanner, J. (2007) Estonia Moves Soviet Statue to Cemetery. *The Associated Press*, 30 April 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/04/30/AR2007043000478.html

[26] Hollis, D. (2011) Cyberware Case Study: Georgia 2008. *Small Wars Journal*, 6 January 2011. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

[27] Markoff, J. (2008) Before the Gunfire, Cyberattacks. *The New York Times*, 13 August 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0

[28] Keizer, G. (2010) Estonia Blamed Russia for Backing 2007 Cyberattacks, Says Leaked Cable. *Computer World*, 9 December 2010. http://www.computerworld.com/article/2511704/vertical-it/estonia-blamed-russia-for-backing-2007-cyberattacks--says-leaked-cable.html

[29] Landler, M. and Markoff, J. (2007) Digital Fears Emerge After Data Siege in Estonia. *The New York Times*, 29 May 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all

[30] Richards, J. (2009) Denial-of-Service: The Estonian Cyberwar and Its Implications for US National Security. *International Affairs Review*, **18**. http://www.iar-gwu.org/node/65

[31] Hõbemägi, T. (2010) Price of Cyberattacks to Hansabank: 10 Million Euros. *Baltic Business News*, 12 August 2010. http://balticbusinessnews.com/article/2010/12/08/Price-of-cyberattacks-to-Hansabank-10-million-euros

[32] Herzog, S. (2011) Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, **4**, 49-60. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss http://dx.doi.org/10.5038/1944-0472.4.2.3

[33] Crawford, J. (2014) The US Government Thinks China Could Take Down the Power Grid. *CNN.com*, 21 November 2014. http://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/

[34] Lloyd's of London (2015) Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid. Lloyd's Emerging Risk Report-2015. https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf

[35] Liptak, A. (2003) The Blackout of 2003: Lawsuits; Plaintiffs to Face Hurdles Proving Liability. *The New York Times*, 15 August 2003. http://www.nytimes.com/2003/08/15/us/the-blackout-of-2003-lawsuits-plaintiffs-to-face-hurdles-proving-liability.html

[36] Garrison v. Pac. Nw. Bell (1980) 608 P.2d 1206, 1211.

[37] Food Pageant, Inc. v. Consol. Edison Co. (1981) 429 N.E.2d 738, 740.

[38] Singer Co., Link Simulation Sys. Div. v. Baltimore Gas & Elec. Co. (1989) 558 A.2d 419, 428.

[39] Frankel, A. (2012) Can Customers Sue Power Companies for Outages? Yes, But It's Hard to Win. *Reuters.com*, 9 November 2012. http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/

[40] Zhang, Z. (2013) Cybersecurity Policy for the Electricity Sector: The First Step to Protecting Our Critical Infrastructure from Cyber Threats. *Boston University Journal of Science and Technology Law*, **19**, 319-366.

[41] Wei, L., Debaise, C. and Bray, C. (2003) Blackout Exposes Power Companies to Potential Lawsuits. *Dow Jones Newswires New York*, 18 August 2003. http://www.oandb.com/blackoutexposes.html

[42] Venable LLP (2014) The SAFETY Act: Providing Critical Liability Protections for Cyber and Physical Security Efforts. https://www.venable.com/files/Publication/6c0b031e-c2c5-4029-9ac7-13cb1d8c0d07/Presentation/PublicationAttachment/e81d24a3-fc57-4ece-8e1f-179418baf994/The_SAFETY_Act_Providing_Critical_Liability_Protections_for_Cyber_and_Physical_Securi.pdf

[43] Eeckhoudt, L., Gollier, C. and Schlesinger, H. (2005) Economic and Financial Decisions under Risk. Princeton University Press, Princeton.

[44] Huang, C.D., Hu, Q. and Behara, R.S. (2008) An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-Averse Firm. *International Journal of Production Economics*, **114**, 793-804. http://dx.doi.org/10.1016/j.ijpe.2008.04.002

[45] Cook, P. and Graham, D. (1977) The Demand for Insurance and Protection: A Case of Irreplaceable Commodities. *Quarterly Journal of Economics*, **92**, 143-156. http://dx.doi.org/10.2307/1883142

[46] Lucas, D. (2014) Rebutting Arrow and Lind: Why Governments Should Use Market Rates for Discounting. *Journal of Natural Resources Policy Research*, **6**, 85-91. http://dx.doi.org/10.1080/19390459.2013.874106

[47] Stewart, M., Ellingwood, B. and Mueller, J. (2011) Homeland Security: A Case Study in Risk Aversion for Public Decision Making. *International Journal of Risk Assessment and Management*, **15**, 367-386. http://dx.doi.org/10.1504/IJRAM.2011.043690

[48] Stewart, M. and Mueller, J. (2013) Aviation Security, Risk Assessment, and Risk Aversion for Public Decisionmaking. *Journal of Policy Analysis and Management*, **32**, 615-633. http://dx.doi.org/10.1002/pam.21704

[49] Farrow, S. and Scott, M. (2013) Comparing Multi-State Expected Damages, Option Price and Cumulative Prospect Measures for Valuing Flood Protection. *Water Resources Research*, **49**, 2638-2648. http://dx.doi.org/10.1002/wrcr.20217