Risk Management Using Cyber-Threat Information Sharing and Cyber-Insurance

Deepak K. Tosh[1(✉)], Sachin Shetty[2], Shamik Sengupta[3], Jay P. Kesan[4], and Charles A. Kamhoua[5]

[1] Department of Computer Science, Norfolk State University, Norfolk, VA, USA
dktosh@nsu.edu
[2] Virginia Modeling Analysis and Simulation Center, Old Dominion University, Virginia, VA, USA
sshetty@odu.edu
[3] Department of Computer Science and Engineering, University of Nevada, Reno, NV, USA
ssengupta@unr.edu
[4] College of Law, University of Illinois, Urbana Champaign, IL, USA
kesan@illinois.edu
[5] Cyber Assurance Branch, Air Force Research Laboratory, Rome, NY, USA
charles.kamhoua.1@us.af.mil

Abstract. Critical infrastructure systems spanning from transportation to nuclear operations are vulnerable to cyber attacks. Cyber-insurance and cyber-threat information sharing are two prominent mechanisms to defend cybersecurity issues proactively. However, standardization and realization of these choices have many bottlenecks. In this paper, we discuss the benefits and importance of cybersecurity information sharing and cyber-insurance in the current cyber-warfare situation. We model a standard game theoretic participation model for cybersecurity information exchange (CYBEX) and discuss the applicability of economic tools in addressing important issues related to CYBEX and cyber-insurance. We also pose several open research challenges, which need to be addressed for developing a robust cyber-risk management capability.

Keywords: Cybersecurity information sharing · Cyber-insurance · Cyber-threat intelligence · Cyber Security Information Sharing Act (CISA)

1 Introduction

Despite the enormous efforts from security researchers, government agencies, and industries toward developing robust security solutions, intelligent adversaries

Approved for Public Release; Distribution Unlimited: 88ABW-2017-2157, Dated: 04 May 2017. This work was supported by Office of the Assistant Secretary of defense for Research and Engineering (OASD (R&E)) agreement FA8750-15-2-0120, Department of Homeland Security Grant 2015-ST-061-CIRC01 and National Science Foundation (NSF) Award #1528167.

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2017
L. Duan et al. (Eds.): GameNets 2017, LNICST 212, pp. 154–164, 2017.
DOI: 10.1007/978-3-319-67540-4_14

find their way in with advanced exploits. Cyber breaches have expanded their breadth not only in the financial sector but also in healthcare, government, educational, defense, and transportation sectors. It was reported that 75% of top 20 financial corporations (banks) are affected by various malwares [1] and some instances include 2014 JP Morgan Data Breach, 2012 DDoS attacks and 2016 SWIFT hack [2]. Losses due to cyber crimes are increasing at an alarming rate and expected to reach $6 trillion by 2021 [3].

In order to abate the impacts of cyber attacks, the organizations, governments, and policy makers are investigating the criticality of ongoing cyber war and proposing mechanisms to effectively defend cyber attacks. The Cybersecurity National Action Plan (CNAP) from U.S. government was proposed in the year 2016 to come up with long-term strategies for fostering cybersecurity awareness, maintain public safety, and protect privacy. The initiative includes establishment of national cybersecurity commission, modernizing government IT infrastructure, and invest more than $19 billion toward cybersecurity research [4]. Besides the efforts from federal level, it must be a customary to adopt best cybersecurity practices at an organizational/individual level. Thus, organizations require the most up-to-date information about attack incidents so as to take proactive measures toward fostering security awareness and better understanding the threat landscape. Since the intelligent attackers can tactfully modify the existing exploits and reuse these exploits for attacking multiple targets, the organizations must collaborate with each other by sharing their vulnerability related information to derive Cyber-Threat Intelligence (CTI) for preventing similar cyber attacks that another firm might have already seen. The bill from U.S congress, "S.754-Cybersecurity Information Sharing Act (CISA) of 2015" [5], encourages DHS to develop a sharing process to facilitate real-time exchange of threat indicators and defensive measures [6] in an automated manner. The bill also provides liability protections to the volunteering parties who share their threat information with other entities or government.

Despite this initiative and advantages of cyber-threat information sharing, organizations are hesitant to take part in such process due to several reasons: (1) lack of trust on the incident exchange process since it may enable competitive advantage to the rivals in the market; (2) possibilities of privacy leak including personal and financial data during the process of sharing that may lead malicious participants to exploit the trust relationship; (3) absence of standardized sharing platform on which organizations can rely upon; (4) insecure feeling of organization to participate in the framework due to the fear of reputation loss; (5) absence of incentivization models to attract corporations toward sharing cybersecurity information; (6) possibility of free-riding, where other organizations take advantages of the shared information without giving anything in return. For availing a globally common format for cyber-information sharing, ITU-T (International Telecommunication Union-Telecommunication) has taken the initiative to adopt a framework called CYBersecurity information EXchange (CYBEX) [7]. However, the framework does not address the fundamental issues, such as trust agreements, governance, or any non-technical aspects, of information sharing.

By addressing these challenges, it can be expected that organizations would be inclined to participate in the threat exchange process so as to strengthen their proactive defense capabilities. At the same time, participation may bring positive externality effect and thereby reducing the investments toward cyber-insurance and self-security expenses.

In this paper, we investigate the need of both cyber-insurance and cybersecurity information sharing in developing a resilient cyberspace for the organizations. We provide the motivations and incremental progresses in this area over the recent past years and discuss how economic models are applicable in addressing several crucial problems related to cyber-insurance and CTI sharing. Given the organizations could reap real-time cyber-related knowledge out of the sharing capability, we discuss how an organization's participation decision can be captured using game theoretic approach. Also, we provide a 2-player game model that aims to resolve the trade-off of deciding whether to participate in CYBEX and share or not. We also present several other research challenges that are yet to be addressed.

The paper is organized as follows. We briefly discuss about the background research in Sect. 2. Need of cyber-insurance and cybersecurity information sharing is presented in Sect. 3. Section 4 presents a sample participation game model and some open research challenges are posed in Sect. 5. Finally, Sect. 6 concludes the paper.

2 Related Works

This topic has gained significant attention and is being investigated by government, policy makers, economists, non-profit organizations, industries, cybersecurity and network professionals with researches in this particular area still emerging [8–10]. Considering the need of cybersecurity information sharing, Gordon et al. [11] analyzed the economic (dis)advantages of this activity and derived its relationship with accounting aspects of an organization Through game theoretic model, they prove that such exchange activity improves the social welfare as well as security level of the firms at a reduced expenditure. Furthermore, an incentive mechanism is provided to eliminate the free-rider problem so that no firm can gain more by making under-investment. It is trivial that nature of information plays a major role in deciding economic losses of an organization, however this component was not addressed in [11]. Authors of [12] have proposed a similar game theoretic model to determine the IT security investment levels and compare it with the outcome of a decision theoretic approach that considers various components, such as vulnerability, payoff from investment etc.

Organizations, especially small scale enterprises, are bounded by a limited budget toward cybersecurity, which is why it is necessary to determine the impact of CTI sharing on the investments altogether. Therefore, authors in [13,14] study to determine the optimal expenditure amount in presence of cyber-information exchange that assists organizations in maximizing their overall payoff. Research works presented in [15,16] have looked into this problem by considering a centralized social planner that guides the organizations in choosing the above mentioned

decision parameters so as to maximize their social welfare. Departing from the traditional inter-networked cyber users, authors of [17] model a non-cooperative game to analyze decision of security investment and information sharing in cloud computing domain, where virtual machines reside on a common hypervisor and there exists possibility of side-channel attacks.

On the other hand, cyber-insurance market is emerging [18] due to the high occurrence of targeted cyber breaches over the years. However, the components such as interdependent security, correlated risks, and information asymmetries [19,20] make it challenging to model appropriate policies for the organizations. Nash equilibrium analysis and social optima concepts are applied to model security games in [21] that consider above three components into account and decide how investment can be used for both public good (protection) and a private good (insurance). Full insurance and partial insurance coverage models are proposed in [22] and study the impact of cooperation on self-defense investments. Another quantitative framework is proposed in [23] that applies optimization technique to provide suggestions to the network users and operators on investments toward cybersecurity insurance by minimizing the overall cyber risks. Although both of the risk reduction strategies are promising in nature there are several avenues that are untouched and yet to be explored.

3 Information Exchange for Balancing Privacy and Security in Cyber-insurance Market

Cyber-insurance preserves market autonomy and is designed to provide coverages for insureds experiencing losses from cyberspace incidents. The premiums for coverages are determined based on insurance applicants underwriting characteristics, which are the key factors chosen by insurers as indicators of applicants risk levels. The cyber-insurance market is characterized by volatile revenue growth, high demand, low capacity and covered loss is much smaller than total loss. However, the unique issue that many cyber-insurance providers are facing is that information regarding the insured is very opaque to insurers and the link

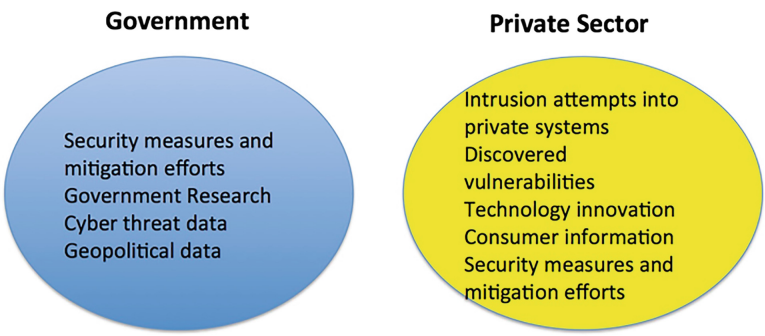

Fig. 1. Public private partnership

between cyber-incidents and financial losses is not well established. There is a lack of quantitative cyber risk assessment and a lot of underwriting is done based on results from questionnaires and interviews [24].

The need to balance privacy and security for facilitating the sharing cyber incidents has generated several debates of legal policy. Private information is held by both the private and public sectors separately and secured to the maximum extent. Any information sharing framework should consider the categories of private information held by both sectors, and the information-sharing program would be narrowly tailored to emphasize the categories of information that would be the most useful to the other side for improving cybersecurity, while excluding the categories of information that would put privacy or national security at risk. Figure 1 illustrates current status of open information sharing [24] and the possible future of open information sharing under a regime like CISA.

Figure 1 illustrates examples of types of information that the different sectors might wish to keep secret [24]. However, in the interest of national security, some types of information would routinely be withheld. For example, while an agency may be forthcoming about recent attempts to hack into its systems, it may be a bad idea to give too much information about the specific vulnerability that was exploited. A privately owned utility company might benefit from information about the vulnerability, but the current paradigm does not have an efficient mechanism for public-private cooperation in cyber-threat information sharing. Information in the right circle could be accessible to the government through existing legal processes. The reluctance to share may be because it could harm a company's reputation or make them into a more attractive target for hackers. This is a major reason why we encourage an organized and largely anonymized system for exchange of vulnerabilities and intrusions.

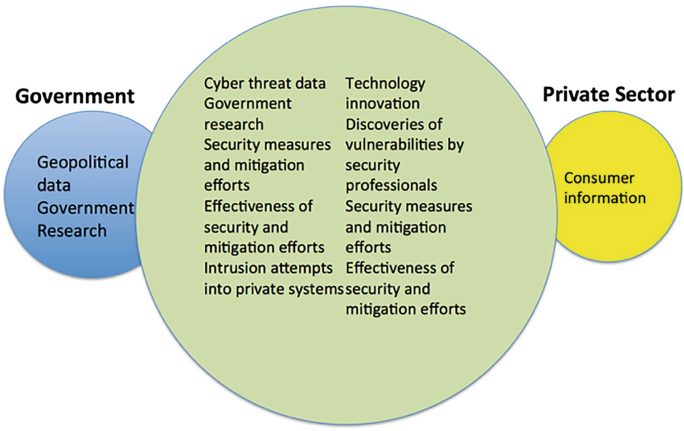

Fig. 2. Conceptual illustration for sector-wide information sharing

Figure 2 illustrates the conceptual illustration for combining the right types of private information without overshare to create a circle of trust [24]. We characterize the middle circle of Fig. 2 as representing a circle of trust managed by a trusted third party. As visualized in Fig. 2, this conceptual illustration would maintain government secrecy for classified military activities and geopolitical information, and would maintain private market secrecy for consumer information, including information about consumers' online activities. In the middle oval, we have placed the types of information that we think could provide the clearest benefits to each sector when shared. Private cybersecurity researchers could benefit from information about intrusion attempts and details about vulnerabilities uncovered by government actors. Government agencies could benefit from up-to-date information about private cybersecurity innovations and the identification of vulnerabilities by private firms. Both sides could benefit from information about different security measures and their rate of success. Some existing laws would need to be revised to implement this proposal, such as the Electronic Communications Privacy Act, which currently may limit the ability of security researchers to share information between firms or with the government.

4 Game Theoretic Model of CYBEX Participation

This Section presents a game model to demonstrate how cybersecurity decisions of interacting organizations are addressable using economic analysis. Despite of understanding the benefits of CTI sharing, most of the organizations are not so motivated to take the risk of participating in CYBEX. Thus, the participation decision requires to be resolved using a cost-benefit approach.

CYBEX Participation Game Model [25]:

In this model, a pair of rational organizations interact with each other to decide whether to participate in the CYBEX or not. Here, CYBEX is a governing entity in the system that imposes participation costs/incentives on the firms to induce participation. The necessity of game theory comes to resolve the following hidden conflict. If CYBEX charges high participation cost, the firms may get deterred from participation, eventually reducing CYBEX's revenue. Whereas, if CYBEX charges too low to attract firms, the revenue generated by CYBEX might be insufficient to sustain in the market. The generic payoff model for organizations must include following two components.

Sharing and Investment Gain: Since organizations are assumed to invest for their own cybersecurity R&D, and infrastructure (firewall, antivirus, and other security products), they receive a direct benefit in term of reduced amount of cyber attacks. Furthermore, the organizations also take advantage of the shared information that leads to additional sharing benefit, which helps to strengthen a firm's proactive cyber-defense capabilities. Subjectively, this benefit comes out of the assistance in strengthening an organization's proactive defense from the received information about vulnerabilities, patches, and fixes.

Cost Components: The involvement in CYBEX requires a participation cost that is imposed by CYBEX to maintain and restrict its utilization by providing liability protections to the firms. In addition to that, sharing of cyber-information has a cost associated which may refer to the combination of extra efforts needed in preparing the information to share and reputation loss incurred due to sharing.

Participation Game in Strategic Form: The participation game can be formalized in a strategic form presented in Table 1, where each firm has the binary strategy set $\mathcal{SS} = \{\text{Participate and Share in CYBEX}, \text{Not Participate}\}$.

Table 1. Payoffs in strategic-form for participation game

	Participate & Share	Not Participate
Participate & Share	$Sa\log(1+I)-x-c$, $Sa\log(1+I)-x-c$	$a\log(1+I)-x-c$, $a\log(1+I)$
Not Participate	$a\log(1+I)$, $a\log(1+I)-x-c$	$a\log(1+I)$, $a\log(1+I)$

From the Table 1, we can observe that when the interacting organizations are not participating, their benefits come only from the self-investment, which is presented in a logarithmic variant, $a\log(1+I) > 0$, where I is the investment amount and a is a scaling parameter. When both organizations take part in the information exchange, they benefit from sharing as well as self-investment but at a cost of participation (c) and information sharing (x). The combined reward is $Sa\log(1+I)$, where S represents the sharing benefits and assumed to be greater than 1. The top-right and bottom-left corners of the table refers to the payoff scenario when one of the organization does not participate while other one does. Thus, the one who is not participating gets reward only out of its own investment, while the participating firm pays for the participation and sharing but gets no sharing benefits in return.

Analysis: By conducting best response analysis, we can observe that irrespective of what strategy the row player takes, the column player's best strategy depends on the choice of sharing benefits (S) and the cost components. Thus, if cost of participation and sharing dominates the total reward, then organizations will preferably opt for the risk averse strategy of "Not Participate". Then, the Nash Equilibrium (NE) solution of the single-shot game will be ("Not Participate", "Not Participate"). However, the single stage scenario does not apply in practice, rather the organizations take time to figure out the long term optimal strategy. Considering the CYBEX is interested in enabling full participation in the system, incentives are necessary to motivate the players to participate. The detailed analysis of such multistage evolutionary model along with incentivization scheme is given in our prior work [26]. However, we feel that this research needs further extension by relaxing some of the natural constraints assumed in

the prior works. In the following, we briefly discuss on various avenues to broaden the scope of this model.

Discussions: The extension ideas are numerated in the following. (E1) In the above model, it is assumed that the organizations have a fixed investment toward security. However, in reality such assumption may not hold true. Therefore, it would be interesting to analyze the participation scenario, when organizations have a differentiated cyber-investments and the amount of information sharing is no longer homogeneous. (E2) The cost of information sharing may not be straightforward as it is depicted in the game, rather a concrete cost model with consideration of attack possibility and privacy would make the case more realistic. (E3) Since some organizations may not be truthful regarding their sharing, this fact will impact the overall participation in the system. Therefore, rigorous analysis is necessary to understand the limits and bounds of maliciousness during information exchange to ensure sustainability of the sharing system.

5 Open Research Challenges

Besides the above directions to extend the CYBEX participation model, there are several challenges exist, which indirectly affect the information sharing decisions of organizations. In the following, we briefly discuss some of these issues.

– **Insurance based mechanism for information sharing:** The participation cost may exhibit the characteristics of insurance which may be a cost or incentive and can be used to motivate socially optimal sharing behavior (through "carrot" incentives like liability protections). However, due to the limited academic literature on cyber-insurance, understanding the effectiveness of cyber-insurance as an incentive/deterrence to induce sharing behavior has become challenging. Also, it is required to know, how long incentives may be applied to develop the sharing attitude without any external incentive.
To model cyber-insurance, the coverage and premium for the insurance will depend on the sharing level, frequency of cyber attack, and attack severity level. As the frequency of attack increases the premium for the insurance gets incremented compared to previous cycle, however periodically the premium amount decreases depending on how successfully the an organization strives against cyber attacks with the help of cooperation. In the following we present a direction toward premium function $C_{prm}(t)$ which can be used to model the expected premium amount that an organizations need to pay towards insurance.

$$C^t_{prm} = \begin{cases} C^{t-1}_{prm} - \delta^{-\alpha_1 t} & \text{if no attack until t and } C^{t-1}_{prm} \geq C_{thres} + \delta^{-\alpha_1 t} \\ C^{t-1}_{prm} + \delta^{\frac{\alpha_2 d}{t_{diff}}} & \text{if attack occured at } t \end{cases}$$

where t_{diff} is the time gap between current time and the last occurrence of cyber attack, δ is the premium exponent defined by the insurance provider, d

is the severity level of the cyber attack and $C_{thres} > 0$, is the min. mandatory premium amount that must be charged to an organization by the insurance agency. $C^0_{prm} = c_0$ is the initial premium amount decided by mutual understanding of both organization and insurance company.

Two primary challenges in designing such a cyber-insurance mechanism are (i) uncertainty (incomplete information) about the information disclosure and (ii) enforcing truthfulness on information exchange, especially in the case when each organization pays differently based on their reliability and reputations.

- **CYBEX with incomplete information:** What if the firms have only partial or incomplete information in this game? How will the competition evolve if some common information now varies or only an estimate is available to all the players in this game? Thus, it becomes important to also consider these assumptions in while making sharing decisions. While, in the above scenario, we emphasized on fixed investment and "participation" vs. "no participation" with pure strategy, it also becomes necessary to extend the game model to consider possibility of continuous domain of investment ($0 < I_i < I_{max}$) as well as mixed strategy for the firms' participation inclination depending on their feedback from the previous stages and payoffs.
- **Measuring cyber risk:** Cyberinsurance has been recognized as an effective way to improve resilience because it speeds up the process of recovery from financial losses after major cyber attack incidents. It also serves as a complement to self-protection as it creates financial incentives for the insured to mitigate cyber-risks in their systems. The cyberinsurance market is premised on being able to develop a comprehensive understanding and assessment of cyber risk. Lack of measurable cyber risks will hinder the ability to develop policies commensurate with the risk profile.
- **Information asymmetry (Adverse selection):** Companies with poor self protection need insurance to have risks covered. However, it is difficult to distinguish the companies with different self-protection and cyber-risks. There needs to be incentive for companies to share such information. If not, insurer will charge premium based on high risk standard to reduce losses. Thereby, the expensive premium will drive away low-risk companies, which will eventually lead to remaining policies in insurer's portfolio filled with bad risk pooling.
- **Information asymmetry (Moral hazard):** Upon receiving coverage, the policyholder may alter its risk characteristics by reducing self-protection to cut cost. After a loss event, policyholder may ask the insurer to pay unnecessary but covered costs. Hence, there are need for game theoretic approaches to address the moral hazard and adverse selection problems.

6 Concluding Remarks

Traditional management of cybersecurity risks requires a strong taskforce and heavy security investment. However, the traditional approaches are more of reactive in nature. Adopting collaborative approach of cyber-threat information sharing could potentially help the organizations to stay on top of the cyber risks.

Furthermore, cyber-insurance could help in transferring risks to the third-party insurers. While both approaches look promising, there exists several research issues that are unresolved. In addition to discussing the advantages these two risk management methods could bring, we have presented the applicability of game theory in addressing CYBEX participation problem. The open research challenges related to these two mechanisms are briefly discussed to further extend the scope of cybersecurity research and particularly CTI sharing.

References

1. https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Financial_Report.pdf
2. https://sentinelone.com/blogs/the-most-devastating-cyber-attacks-on-banks/
3. http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
4. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
5. https://www.congress.gov/bill/114th-congress/senate-bill/754
6. Fischer, E., Liu, E., Rollins, J., Theohary, C.: The 2013 cybersecurity executive order: overview and considerations for congress (2013)
7. Rutkowski, A., Kadobayashi, Y., Furey, I., Rajnovic, D., Martin, R., Takahashi, T., Schultz, C., Reid, G., Schudel, G., Hird, M., Adegbite, S.: Cybex: the cybersecurity information exchange framework (x.1500). SIGCOMM Comput. Commun. Rev. **40**, 59–64 (2010)
8. Wang, T., Kannan, K.N., Ulmer, J.R.: The association between the disclosure and the realization of information security risk factors. Inf. Syst. Res. **24**(2), 201–218 (2013)
9. Dandurand, L., Serrano, O.S.: Towards improved cyber security information sharing. In: 5th International Conference on Cyber Conflict, pp. 1–16. IEEE (2013)
10. de Fuentes, J.M., González-Manzano, L., Tapiador, J., Peris-Lopez, P.: Pracis: privacy-preserving and aggregatable cybersecurity information sharing. Comput. Secur. **69**, 127–141 (2016). doi:10.1016/j.cose.2016.12.011. ISSN 0167-4048
11. Gordon, L.A., Loeb, M.P., Lucyshyn, W.: Sharing information on computer systems security: an economic analysis. J. Acc. Publ. Policy **22**(6), 461–485 (2003)
12. Cavusoglu, H., Raghunathan, S., Yue, W.T.: Decision-theoretic and game-theoretic approaches to it security investment. J. Manag. Inf. Syst **25**(2), 281–304 (2008)
13. Tosh, D.K., Sengupta, S., Mukhopadhyay, S., Kamhoua, C., Kwiat, K.: Game theoretic modeling to enforce security information sharing among firms. In: IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 7–12 (2015)
14. Tosh, D.k., Molloy, M., Sengupta, S., Kamhoua, C.A., Kwiat, K.A.: Cyber-investment and cyber-information exchange decision modeling. In: IEEE 7th International Symposium on Cyberspace Safety and Security, pp. 1219–1224 (2015)
15. Hausken, K.: A strategic analysis of information sharing among cyber hackers. JISTEM-J. Inf. Syst. Technol. Manag **12**(2), 245–270 (2015)
16. Gal-Or, E., Ghose, A.: The economic consequences of sharing security information. Econ. inf. secur **12**, 95–105 (2004)
17. Kamhoua, C., Martin, A., Tosh, D.K., Kwiat, K., Heitzenrater, C., Sengupta, S.: Cyber-threats information sharing in cloud computing: a game theoretic approach. In: IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 382–389 (2015)

18. http://www.businessinsurance.com/article/20161207/NEWS06/912310865/Cyber-insurance-market-to-grow-says-Allied-Market-Research
19. Anderson, R., Moore, T.: The economics of information security. Science **314**(5799), 610–613 (2006)
20. Böhme, R., Schwartz, G., et al.: Modeling cyber-insurance: towards a unifying framework. In: WEIS(2010)
21. Grossklags, J., Christin, N., Chuang, J.: Secure or insure?: a game-theoretic analysis of information security games. In: Proceedings of the 17th international conference on World Wide Web, pp. 209–218. ACM (2008)
22. Pal, R., Golubchik, L.: Analyzing self-defense investments in internet security under cyber-insurance coverage. In: 2010 IEEE 30th International Conference on Distributed Computing Systems (ICDCS), pp. 339–347. IEEE (2010)
23. Young, D., Lopez, J., Rice, M., Ramsey, B., McTasney, R.: A framework for incorporating insurance in critical infrastructure cyber risk strategies. Int. J. Crit. Infrastruct. Prot. **14**, 43–57 (2016)
24. Kesan, J.P., Hayes, C.M.: Creating a circle of trust to further digital privacy and cybersecurity goals, Mich. St. L. Rev., p. 1475 (2014)
25. Tosh, D.K., Sengupta, S., Kamhoua, C.A., Kwiat, K.A., Martin, A.: An evolutionary game-theoretic framework for cyber-threat information sharing. In: IEEE International Conference on Communications, ICC, pp. 7341–7346 (2015)
26. Tosh, D., Sengupta, S., Kamhoua, C.A., Kwiat, K.A.: Establishing evolutionary game models for cyber security information exchange (CYBEX). J. Comput. Syst. Sci. (19 October 2016). doi:10.1016/j.jcss.2016.08.005. ISSN 0022-0000