Contents lists available at ScienceDirect

European Journal of Operational Research

journal homepage: www.elsevier.com/locate/ejor

Production, Manufacturing and Logistics

Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability

Anna Nagurney*, Shivani Shukla

Department of Operations and Information Management, Isenberg School of Management, University of Massachusetts, Amherst, MA 01003, United States

ARTICLE INFO

Article history:
Received 13 April 2016
Accepted 22 December 2016
Available online xxx

Keywords:
Cybersecurity
Investments
Game theory
Nash equilibrium
Nash bargaining

ABSTRACT

In this paper, we develop and compare three distinct models for cybersecurity investment in competitive and cooperative situations to safeguard against potential and ongoing threats. We introduce a Nash equilibrium model of noncooperation in terms of cybersecurity levels of the firms involved, which is formulated, analyzed, and solved using variational inequality theory. The equilibrium of this model then acts as the disagreement point over which bargaining takes place in the setting of the second model, which yields a cooperative solution in which the firms are guaranteed that their expected utilities are no lower than those achieved under noncooperation. Nash bargaining theory is utilized to argue for information sharing and to quantify its monetary and security benefits in terms of reduction in network vulnerability to cyberattacks. The third model in this paper also focuses on cooperation among the firms in terms of their cybersecurity levels, but from a system-optimization perspective in which the sum of the expected utilities is maximized. Qualitative properties are provided for the models in terms of existence and uniqueness results along with numerical solutions to two cases focusing on retailers and financial service firms, since these have been subject to some of the most damaging cyberattacks. Sensitivity analysis results are also provided. We compare the solutions of the models for the cases and recommend a course of action that has both financial and policy-related implications.

1. Introduction

The effects of cyberattacks are being felt across the globe in multiple sectors and industries. The damages incurred include direct financial damages as well as reputation issues, the loss of business, the inability to provide the expected services, opportunity costs, and the loss of trust. According to the Center for Strategic and International Studies (2014), the world economy sustained 445 billion dollars in losses from cyberattacks in 2014. The United States suffered a loss of 100 billion dollars, Germany lost 60 billion dollars, China lost 45 billion dollars, and the United Kingdom reported a loss of 11.4 billion dollars due to cybersecurity lapses. The think tank also presented an analysis that indicated that of the 2 trillion dollars–3 trillion dollars generated by the Internet annually, about 15%–20% is extracted by cybercrime. Adversaries in the cyber realm include spies from nation-states who seek our secrets and intellectual property; organized criminals who want to steal our identities and money; terrorists who aspire to attack our power grid, water supply, or other infrastructure; and hacktivist groups who are trying to make a political or social statement (Deloitte, 2014).

The evolving threat landscape of cybercrime heavily targets organizations in energy, retail, financial services, critical manufacturing, communications, and even healthcare. According to the US Department of Homeland Security (2015), the energy sector constituted the highest number of incidents (32%) reported in Fiscal Year 2014. The reality of effects of cyberattacks on energy infrastructure is brought forth by the recent “UglyGorilla” attack in 2014 that sought access to pipeline schematics and natural gas flow regulations systems in the United States through the remote shutdown of critical systems (Bloomberg, 2014a; 2014b). In order to protect the electric grids, and oil and natural gas infrastructure from threats, the Energy Department in October 2015 announced 34 million dollars toward R&D efforts US Department of Energy (2015). The retail sector, on the other hand, has reported to-date one of the biggest breaches with heavy losses. In 2014 alone, Target, Home Depot, Michaels Stores, Staples, and eBay were breached. Card data and personal information of millions of customers were stolen and the detection of cyber espionage became the prime focus for the retail sector with regards to cybersecurity (Granville, 2015). Since financial gains, through the subversion of processes and controls, are

* Corresponding author at: John F. Smith Memorial Professor, Operations & Information Management, 121 Presidents Dr., Amherst, MA 01003, USA, Office: Isenberg 306.

E-mail address: nagurney@isenberg.umass.edu (A. Nagurney).

http://dx.doi.org/10.1016/j.ejor.2016.12.034
0377-2217/© 2016 Elsevier B.V. All rights reserved.

one of the most attractive benefits emerging from cyberattacks, financial service firms are targeted incessantly. The large-scale data breach of JP Morgan Chase, Kaspersky Lab's detection of a two-year infiltration of 100 banks across the world costing 1 dollars billion (USA Today, 2015), and the Dridex malware related losses of 100 million dollars worldwide (Dodd, 2015) are some of the widely accepted cautionary tales in this sector.

According to the Ponemon Institute (2015), the average annualized cost of cybercrime incurred by a benchmark sample of organizations was 15 million dollars. The range of these annualized costs was 1.9 million dollars–65 million dollars, an 82% increase in the past six years. Most of these cybercrimes are generally caused by denial of service, malicious insiders, and malicious code affecting physical and cyber assets. A survey conducted by AON Risk Services and Ponemon Institute (2015) concluded that despite the comparability of the average potential loss to information assets (617 million dollars) and property, plant and equipment (648 million dollars), the percentages of insurance coverage are 51% and 12%, respectively. Moreover, because of the interlinkages among different firms, organizations, institutions, and even nations, due to the Internet and associated advanced technologies, a single firm, organization, nation, or even individual may affect the vulnerability of others to cyberattacks. The technological innovations that are being envisioned could intensify these losses even more as they introduce new entry points for cyberattacks (The Wall Street Journal, 2014). These inclement costs ultimately trickle down to organizations and consumers.

For example, the Internet of Things (IoT) has expanded the possible entry points for cyberattacks (ComputerWeekly.com, 2015). According to McKinsey Company Quarterly (2014), worries about cyberattacks are beginning to have quantifiable negative business implications. In high tech, half of the McKinsey executives surveyed said they would modify the characteristics of their R&D efforts over time with added concerns that cyberattacks could slow down the capture of value creation from cloud computing, mobile technologies, and healthcare technologies. As reported therein, 70% of the respondents noted that security concerns had delayed the adoption of public cloud computing by a year or more, and 40% said that because of such concerns enterprise-mobility capabilities were delayed by a year or more.

The increased rate of cyberattacks has spurred the behavioral analysis of attackers and defenders. Aggarwal et al. (2015) take a game theory approach to study actions of attackers and defenders in a 2 × 4 cybersecurity game that is evaluated computationally through 1000 simulations. A defense exercise model using game theory is developed by Patrascu and Simion (2014) to train cyber response specialists. Nagurney (2015) utilized a network economics approach to model cybercrime emphasizing that both firms and hackers act as economic agents. RAND Security Division (2014) also argued that an economic approach to tackling cybercrime is warranted.

In addition to investigating interactions among attackers and defenders, there has also been a growing literature on cybersecurity investments. The investment in cybersecurity through software and hardware, education, and effective personnel can help resist the growing frequency and severity of attacks, and assist in the planning of appropriate allocation of resources required to prevent/mitigate the likely damage. Garvey, Moynihan, and Servi (2013) suggested an approach that helps to prioritize among competing investment options for better cyber defense. They identify sets of Pareto efficient cost-benefit investments, and their economic returns, that capture tangible and intangible advantages of countermeasures that strengthen cybersecurity. From a social welfare standpoint, Gordon, Loeb, Lucyshyn, and Zhuo (2015) examined changes in the maximum a firm should invest into cybersecurity activities in the face of well-recognized externalities.

Nevertheless, the domain of security in computer networks has a limited but useful literature employing game theory. Zero-sum, non-zero-sum, dynamic, stochastic, repeated, Stackelberg, static, and coalition games have been applied to computer and communication networks. Manshaei, Alpcan, Basar, and Hubaux (2013) provide a survey of the literature combining game theory and security. The survey is divided into six main categories: security of the physical and MAC layers, security of self-organizing networks, intrusion detection systems, anonymity, and privacy, the economics of network security, and cryptography. Das (2015) presents a cybersecurity ecosystem consisting of network, cloud, and software providers and economically analyzes the risk of correlation between agents in the ecosystem in case of a breach. Shetty, Schwartz, Felegyhazi, and Walrand (2010) and Shetty (2010) focus on game theory for the determination of cybersecurity levels through investments. In both those publications, the authors determine the Nash equilibrium as well as the social optimum associated with security levels. However, it is assumed that the firms face identical cybersecurity investment cost functions, have identical wealth, and also the damages afflicted due to a cyberattack are the same. Nagurney and Nagurney (2015) and Nagurney, Nagurney, and Shukla (2015), inspired, in part, by that research, relaxed the assumptions of identical firms, and further quantify the expected utilities of financial firms/retailers in a bipartite network with investment costs, supply prices, transaction costs, and demand price functions, taking a supply chain perspective. A variational inequality and noncooperative game theoretic approach is utilized to arrive at the equilibrium production quantities and cybersecurity levels given firm and consumer behavior that ultimately ascertain the network vulnerability. A recent edited volume by Daras and Rassias (2015) includes additional information on network security models and frameworks.

Nagurney (2015) emphasized the importance of assessing the vulnerabilities of cyberattacks in a rigorous quantifiable manner and identifying possible synergies associated with information sharing for firms providing critical infrastructure networks on which our economy and society depend. The complexity and interdependence of firms, governments, and individuals in intricately woven networks mean that an attack on one may pave the way for attacks on others. Given that the number and intensity of cyber threats for every industrial and non-industrial sector have increased, firms and governments are progressing toward sharing threat information to arrange coordinated defenses against attacks.

An increasingly connected world may amplify the effects of a disruption. Information Technology (IT) outages of any kind can lead to material losses as well as loss of data, unplanned downtime, and adverse impacts on the reputations of the affected organizations. Firms interacting with one another may be at varied levels of IT and security maturity. Cybersecurity related measures are found mostly at an organizational level. Breaking down these silos and sharing information can have a direct impact on business continuity. This makes security governance an integral part of risk management and business continuity strategies of organizations in the support of their client processes. We suggest that, by taking a network perspective, in evaluating both noncooperative and cooperative behavior in terms of cybersecurity investments, can provide insight into the value of information sharing. Nevertheless, information sharing may have its disincentives since cooperation on the cyber front is being struck between competitors in the market.

In this paper, we present three new models of cybersecurity investments. Our proposed models are not restricted to the number of firms, their locations, or the sectors that they belong to. We begin with a Nash equilibrium model of noncooperation and competition, which is formulated, analyzed, and solved using variational inequality theory. The solution to this Nash equilibrium model then serves as the disagreement point over which the