Proceedings of the 2022 Winter Simulation Conference
B. Feng, G. Pedrielli, Y. Peng, S. Shashaani, E. Song, C.G. Corlu, L.H. Lee, E.P. Chew, T. Roeder, and P. Lendermann, eds.

A DYNAMIC THEORY OF SECURITY FREE-RIDING BY FIRMS IN THE WFH AGE

Ranjan Pal

Department of Computer Science and Technology
University of Cambridge
15 JJ Thomson Avenue
Cambridge CB3 0FD, UK

Rohan Xavier Sequeira
Louise Zhu
Yushi She

Electrical Engineering and Computer Science
University of Michigan
1301 Beal Ave
Ann Arbor, MI 48109, USA

ABSTRACT

The COVID-19 pandemic has radically transformed the work-from-home (WFH) paradigm, and expanded an organization's cyber-vulnerability space. We propose a novel strategic method to quantify the degree of sub-optimal cybersecurity in an organization of employees, all of whom work in heterogeneous WFH "siloes". Specifically, we model the per-unit cost of asymmetric WFH employees to invest in security-improving effort units as time-discounted exponential martingales over time, and derive as benchmark - the centrally-planned socially optimal aggregate employee effort at any given time instant. We then derive the time-varying strategic Nash equilibrium amount of aggregate employee effort in cybersecurity in a distributed setting. The time-varying ratio of these centralized and distributed estimates quantifies the free riding dynamics, i.e., security sub-optimality, within an organization. Rigorous estimates of the degree of sub-optimal cybersecurity will drive organizational policy makers to design appropriate (customized) solutions that voluntarily incentivize WFH employees to invest in required cybersecurity best practices.

1 INTRODUCTION

As economic activities around the globe become pervasively digital, the ever-increasing cyber-threat is outpacing most companies' ability to manage it effectively. Sensitive business information, such as employee personal information, client and corporate data, and intellectual property all are at an increasing risk of getting hacked. Along with them, other key elements of corporate infrastructure are also under growing threat from ransomware risks. Commercial cyber-risk management activities such as ID theft resolution and credit monitoring have become ubiquitous all over the globe thanks to countless data breaches since the mid-2000s, and are exploding in the era of smartphone communication. Fast forward to the post 2020 era, phishing scams are running rampant amid COVID-19 that has given rise to the work-from-home (WFH) paradigm. WFH has blurred the distinction between workplace and home environments when it comes to business delivery outcomes. According to *Hewlett Packard*, there has been a stupendous 238 percent increase in global cyber-attack volume during the COVID-19 pandemic. Individuals are waking up to annoying (e.g., loss of private data and digital mementos from the phone) and often serious (e.g., loss of workplace data from the cloud) cyber-risks. This is hardly surprising given the forced choice for employees to work from home, along with security-productivity-lifestyle tradeoffs that accompany this paradigm.

1.1 The Security-Productivity-Lifestyle Tradeoffs of Working from Home

According to the survey analysis expert *KuppingerCole*, many employees believe they are more productive (not necessarily due to an outcome of COVID) when working from home compared to a traditional office

setting, thanks to flexible time-management and time saving benefits. However, quite a few of them - approximately 25 percent believe they are less productive while working from home. This is because in many parts of the world, even in developed countries, high-spec hardware like laptop and tablets, and software like video-conferencing tools and database management systems (DBMSs) require highly reliable and secure internet connection and a secure access to the corporate network via VPN, all of which are not guaranteed if one is working from home. While the governments in collaboration with network providers have been handling the issue of expanding fibre capacity, given the critical importance of cybersecurity in this new WFH setting, employers are steadily putting in place a whole range of efficient cybersecurity measures for this 'new' work environment.

Ensuring efficiency is, however, just one factor involved in IT security measures applied to staff working from home. Another salient factor is the need to prevent cyberattacks, and step number one en route that goal is to know how WFH employees perceive their corporate cybersecurity posture. According to KuppingerCole, approximately only 14 percent of WFH non-security experts are concerned about cybersecurity when working from home. Furthermore, 25 percent of the non-security experts report an increase in fraudulent emails, phishing attempts, and spam to their corporate email since the start of the COVID-19 crisis — this excludes cyber-attacks that have gone unrecognised. Hence, the underlying message here is that *there is anecdotal evidence from businesses that the COVID-19 pandemic has triggered a change of tactics used by cyber criminals who are now attempting to exploit weaknesses of remote IT security.* So the major question here then becomes: *what are these WFH-specific cybersecurity weaknesses that have cyber-criminals drooling to compromise corporates?*

1.1.1 Surveyed WFH cybersecurity Weaknesses

Most employees in the WFH mode agree that they access more company data, and at a higher frequency, than they did pre-pandemic. The most common types of data accessed, according to KuppingerCole, is customer and operational data, 43% each, and financial and HR records, 23% each. A significantly important new dimension specific to WFH is that office workers are increasingly using their work devices for personal tasks today. Based on surveys by leading IT and cyber-consulting firms including HP and Deloitte, approximately 33 percent WFH employees download more from the internet, compared to the pre-pandemic phase, and this statistic rises to 60% for those aged 18-24. Around 27% WFH employees surveyed used their work device to play online games when compared to the times pre-pandemic - a statistic that sharply rises to 43% for parents of children aged 5-16, who were spending more time with their children.

Close to 36% surveyed WFH employees use their work device to watch online streaming services - a figure that steeply rises to 60% among those aged 18-24. Around four in ten office workers used their work device for homework and online learning purposes. This statistic rises to 57% for parents of children aged 5-16. In the age of WFH, cyber-hackers are taking advantage of these shifting patterns of device-task mapping to tailor their phishing campaigns. Globally, there was approximately a 54% increase in malicious actors who exploited gaming platforms between January and June of 2020, and directed users to phishing pages. In strong correlation to this statistic, during this same period, (i) there was an increase in gaming-themed malware such as *Ryuk* ransomware and samples of stealthy JavaScript downloader malware, *Gootloader*, masquerading as *Fortnite* hacks, and (ii) at least 700 fraudulent websites were found to be impersonating popular streaming services in just one seven-day period in April 2020.

In addition to the overlapping of work and personal activities on business devices, WFH office workers are also using potentially insecure personal devices (not protected anymore by corporate firewalls) to connect to their corporate environment. 88% divisional managers of IT departments are worried cyber-breach risk has risen only because employees are using personal devices for work. In addition, approximately half of these managers have enough evidence that compromised personal devices (about 1.5 attacks per minute) are being used to access business data during the ongoing pandemic. According to a *YouGov* survey, for the year 2020, approximately 69% of office employees have used personal laptops, printers, and so on, to

execute corporate tasks more often since the pandemic began. This statistic is further distributed among activities such as using personal PC/laptop for office work (approximately 37%), using personal PC/laptop to access organisational network and servers (about 32%), using personal scanner and printers to share work-related documents with other colleagues (about 34%), and using home printers to save files, through VPN, on the office network (about 20%).

Such activities amplify the already existing cyber-risk posture for firms with respect to client/business data privacy, repetitional damage, non-compliance, and loss of customer trust. Hence, in the WFH age, having strong endpoint security has become equally important to corporate businesses as having strong network security. Even on a psychological level, behavioral research has found that approximately 10% WFH employees reported feeling tired or having little energy or motivation (e.g., missing social interactions with colleagues, distraction by family at home) while working from home, according to Society of Human Resource Management. This is a significant worry factor for corporations simply because tired or unmotivated employees are prone to making careless errors, and such errors could easily trickle into the organisation security space, jeopardising the latter with an increased risk of sensitive information or network compromise. As an example, while working on a sensitive business file (or while configuring DBMS settings) you suddenly realise that you have laundry to pick up and, in a hurry, misplace the confidential document (or misconfigure the DBMS) in the wrong place. To put the importance of human behavior into perspective, a Hewlett Packard *Wolf Security Report* states that in the year 2020, around 82% of office employees did WFH and 39% of them wish to WFH post the pandemic. *Hence, it is not difficult to infer that cyber-risk in the age of WFH is going to significantly increase, compared to the pre-pandemic era.*

1.2 Research Motivation and Contributions

We motivate our research problem and follow it up with a brief outline of our research contributions.

1.2.1 Research Motivation

One of the main contributing factors for the increased cyber-risk an organization will likely face in the WFH age is the heterogeneity and dynamicity in the working environments of its employees (as stated in Section 1.1.1 earlier). This would reflect in the amount of effort towards cybersecurity best practices an individual employee puts in at home conditions - *a quantity that is varying over time, and over the heterogeneous home environments each employee is subject to.* Under this setting, the organization is keen to compare between the best possible cybersecurity state possible - a condition that is most likely to be approximately reached in homogeneous and IT team controlled working environments (such as when most employees are inside the organization), and the state of cybersecurity when individuals are distributed in 'un'-controlled (involves partial control by IT team of an organization) heterogeneous home environments. *The amount of difference in the two states is analogous to the degree of sub-optimal cybersecurity within the organization, and would drive the C-Suite in promoting and investing in appropriate cybersecurity boosting organizational policies for its employees in the WFH age.* One might argue that such differences in 'centralized' vs 'distributed' cybersecurity outcomes have also been of interest to C-Suites in the pre-COVID era. While this is definitely true for some organizations, *the degree of both environment and effort heterogeneity over time is far greater in a WFH scenario to warrant a fresher look to characterizing these differences in a mathematically rigorous fashion for this scenario.*

1.2.2 Research Contributions and Novelty

We model in Section 2, a practically realistic WFH setting for an organization with n employees, where each employee's effort cost to invest in cybersecurity best practices in heterogeneous WFH environments is *time-varying*, *continuous*, and *asymmetric* over the space of employees. In Section 3, we subsequently use this model to derive an optimal centralized time-dependent policy for the organization that serves as a benchmark on how (in terms of optimal effort units) each individual in the organization should invest in

cybersecurity best practices over a finite period of time in a WFH setting. In Section 4, we analyse how strategic but perfectly rational individuals in distributed heterogeneous WFH environments behave over time in terms of investing in cybersecurity efforts. In Section 5, we rigorously quantify the time-dependent dissimilarity in aggregate cybersecurity efforts (over all employees) between the centralized benchmark and distributed scenarios by evaluating their time-varying ratios. These ratios denote the dynamic free-riding extents (dynamic measures of an organization's degree of sub-optimal cybersecurity) experienced by an organizational system when their employees work in heterogeneous WFH environments. The primary novelty of our efforts lies in rigorously characterizing cybersecurity free-riding effects in dynamic and heterogeneous WFH environments. *To the best of our knowledge, there exists no work in the cybersecurity research literature (leave along specific WFH security literature) that formally addresses the quantification of free-riding effects in general but practically realistic time-varying and asymmetric player environments.*

1.3 Related Work

Quantifying free-riding effects in work-from-home (WFH) settings is an un-chartered territory. To the best of our knowledge, there is no existing work on this topic. However, given that WFH security problems necessarily assume cybersecurity to be a public good, we briefly review related work in the topics of (a) free-riding on public goods, and (b) cybersecurity games among rational agents. Free riding analysis of public good games have been proposed in (Olson 1965; Samuelson 1954; Palfrey and Rosenthal 1984; Bergstrom et al. 1986; Groves and Ledyard 1977). *However, these one-shot games are static in nature and does not help capture the dynamic free-riding due to time-varying and asymmetric human efforts in cybersecurity that is actually the case in practice (including WFH settings).* Dynamic games analysing public good free riding have been proposed in (Varian 1994; Fershtman and Nitzan 1991; Levhari and Mirman 1980; Marx and Matthews 2000; Bag and Roy 2011). *However, these games assume a simple environment where player interest of investing in security best-practice efforts is a deterministic varying function over time.* Though this assumption takes a big leap over static game-theoretic models mentioned above, it does not help capture the random changes in the effort-providing environment of asymmetric players that is actually the case in practice (including WFH settings). Dynamic free-riding analyses due to random changes in public-good contributing environments of players have been modeled in (Wang and Ewald 2010; Yeung and Petrosyan 2013) as stochastic differential games using a diffusion term. *However, these works make a Markovian assumption on the modulating process of the diffusion equation that describes state flow - something is does not usually hold true in practice.* We relax this assumption in this work to be more close to real human behavior in WFH settings with respect to investing in cybersecurity effort. Our approach is inspired from public good economic analysis methodologies proposed in (Varian 1994; Ferrari et al. 2017) In the space of security games with positive and negative externalities, there has been a considerable literature (Gordon et al. 2003; Ögüt et al. 2005; Jiang et al. 2010; Varian 2004; Kunreuther and Heal 2003; Grossklags et al. 2008; Grossklags et al. 2010; Hota and Sundaram 2016; Amin et al. 2011; Amin et al. 2013; La 2017; La 2016; Lelarge and Bolot 2008; Pal and Golubchik 2010; Pal and Hui 2011) whose main research essence has been summarized through a survey in (Laszka et al. 2014). *However, all these efforts are (mostly one-shot static) game models and does not capture dynamic free-riding and time-varying asymmetric human efforts in cybersecurity characterizing WFH settings in practice.*

2 A TIME-VARYING EFFORTS MODEL OF ASYMMETRIC WFH EMPLOYEES

In this section we model asymmetric employees in practically realistic WFH settings, where the asymmetry is with respect to their time-varying propensity to invest in efforts promoting cybersecurity best practices for their organization.

We consider an organization with a finite number $n \geq 1$ of employees adopting the work-from-home (WFH) paradigm over a fixed time horizon $0 < T \leq \infty$. An example of such a time horizon is a COVID-induced lockdown period during which the organizational employees are mandated to work from home.

Each employee, indexed by $i = 1, \ldots, n$, chooses how to allocate his total effort budget $w^i > 0$ (a product of effort and a psychological cost per unit of effort - see details below) during the period of duration T between (a) effort, x^i, towards work and family activities, and (b) arbitrary but non-decreasing cumulative contributions, C^i, to efforts in ensuring cybersecurity best practices set by the organization (e.g., by the IT managers such as CIOs and CISOs), thereby adding to the level of cybersecurity as a public good. We assume a continuous and exogenous source of uncertainty related to the propensity of WFH employees to invest in cybersecurity best practices. As an example, for two different time instants t and t' in $[0,T]$, the propensity for employee i to invest in security practices could be randomly (non-deterministically) varying due to factors such as behavioral biases, mood at home, family commitments during work hours etc. Formally, let $(\Omega, \mathscr{F}, \{\mathscr{F}_t\}_{t\in[0,T]}, \mathbf{P})$ be a filtered probability space satisfying the usual conditions of right-continuity and completeness. We do not make any Markovian assumption.

At any given time t in $[0,T]$, each WFH employee can invest in multiple effort units in work and family activities at a price of $\psi_x(t)$ per unit of effort. This price reflects the psychological propensity of employees to contribute to their work and family activities - higher the price, lesser the propensity and vice versa. We assume the price randomly varies over time, again due to factors such as behavioral biases, mood at home, family commitments during work hours etc. The adapted process $\psi_x := \{\psi_x(t), t \in [0,T]\}$ is right-continuous (follows from a right-continuous version of the exponential martingale $\mathscr{E}_c$, and is uniformly integrable) and such that $\psi_x(t) = e^{-\int_0^t r_x(s)ds}\mathscr{E}_x(t)$ a.s. for every $t \in [0,T]$, with some uniformly bounded and strictly positive process $r_x := \{r_x(t), t \in [0,T]\}$ and some exponential martingale $\mathscr{E}_x := \{\mathscr{E}_x(t), t \in [0,T]\}$. Analogously, the contingent price for the contribution to the cybersecurity public good is $\psi_c(t)$. The adapted process $\psi_c := \{\psi_c(t), t \in [0,T]\}$ is right-continuous (follows from a right-continuous version of the exponential martingale $\mathscr{E}_c$, and is uniformly integrable) and such that $\psi_c(t) = e^{-\int_0^t r_c(s)ds}\mathscr{E}_c(t)$ a.s. for every $t \in [0,T]$, with some uniformly bounded and strictly positive process $r_c = \{r_c(t), t \in [0,T]\}$ and some exponential martingale $\mathscr{E}_c := \{\mathscr{E}_c(t), t \in [0,T]\}$. Moreover, if $T = \infty$, one has $\psi_c(T) = 0$ a.s. ψ_x and ψ_c are strictly positive, and the optional, strictly positive process $r := \{r(t), t \in [0,T]\}$ is uniformly bounded. Assuming exponential martingales for stochastic processes characterizing ψ_c and ψ_x makes them positive.

The total cost incurred by WFH employee i over $[0,T]$ on a cybersecurity investment plan (x^i, C^i) is

$$\Psi(x^i, C^i) := \mathbb{E}\left[\int_0^T \psi_x(t)x^i(t)dt + \int_0^T \psi_c(t)dC^i(t)\right],$$

where, the pair of time-varying functions (x^i, C^i) lie in the nonempty, convex budget-feasible set

$$\begin{aligned}\mathscr{B}_{w^i} := \Bigg\{ &(x^i, C^i) \colon \Omega \times [0,T] \mapsto \mathbb{R}^2_+ \text{ optional, s.t. } C^i \text{ is right-continuous and nondecreasing} \\ &\text{with } C^i(0-) = 0 \ \mathbf{P}\text{-a.s., and } \mathbb{E}\left[\int_0^T \psi_x(t)x^i(t)dt + \int_0^T \psi_c(t)dC^i(t)\right] \le w^i \Bigg\}.\end{aligned} \tag{1}$$

Here, a stochastic process is *optional* Dellacherie et al. (1978) if it is measurable with respect to the optional sigma-field $\mathscr{O}$ on $\Omega \times [0,T]$ generated, e.g., by the right-continuous adapted processes (any optional process is adapted and right-continuous). The quantity $\Psi(x^i, C^i) \le w^i$ reflects the budget constraint of WFH employee i. Notice that the definition of C^i allows jumps as well as singular increases (with respect to the Lebesgue measure). This means that employees can contribute to cybersecurity best practices both in lumps at certain times (e.g., when psychologically motivated to), and also continuously (e.g., as part of work routine), the latter even not necessarily in rates. Note that since each $t \mapsto C^i(t)$ is a.s. non-decreasing, we can denote by $\int_0^T (\cdot)\, dC^i(t)$ the Lebesgue-Stieltjes integral $\int_{[0,T]} (\cdot)\, dC^i(t)$ throughout, to include the possibility of initial jumps in the efforts towards ensuring security best practices, corresponding to a point mass $C^i(0) > 0$ of the random Borel measure dC^i at time $t = 0$.

We assume that the WFH employees gather some expected, time-separable utility from effort investments in work and family life, and also from those that contribute to the aggregate cybersecurity public good

(that generates externalities) $C := \sum_{i\in\{1,\dots,n\}} C^i$ contributed by all the WFH employees of the organization. Given a combination of strategies from $\prod_{i=1}^n \mathscr{B}_{w^i}$, employee i's expected utility (payoff) is given by

$$U^i(x^i, C^i; C^{-i}) := \mathbb{E}\left[\int_0^T e^{-\int_0^t r(s)\,ds} u^i(x^i(t), C(t))\,dt\right], \tag{2}$$

where $C^{-i} := \sum_{j\in\{1,\dots,n\}\setminus i} C^j$, r is an exogenous stochastic discount factor and $u^i : \mathbb{R}^2_+ \mapsto \mathbb{R}_+$ is an instantaneous utility function. In this paper, we work with general strictly concave utilities for the WFH employees. More specifically, we assume that for each WFH employee u^i is increasing and strictly concave on $\mathbb{R}^2_+$, and twice continuously differentiable on the open cone $\mathbb{R}^2_{++}$, with a negative definite Hessian. In addition the following boundary *Inada* conditions (Takayama and Akira 1985) hold for u^i

$$\lim_{x\downarrow 0} u^i_x(x,c) = +\infty \quad \text{and} \quad \lim_{x\uparrow\infty} u^i_x(x,c) = 0$$

for any $c > 0$. The first Inada condition states that the limit of the first derivative of $u^i_x(x,c)$ is infinity as the effort amount invested in work and family matters, x^i, approaches zero. In practice, this reflects the fact that the marginal positive utility effect to the WFH employee of it investing one additional unit of effort x^i to work and family matters is very high if there has been no prior investments made on that front by the WFH employee. On the contrary, the second Inada condition states that the limit of the first derivative of $u^i_x(x,c)$ is zero as the effort amount invested in work and family matters, x^i, approaches infinity. In practice, this reflects the fact that the marginal positive utility effect to the WFH employee of it investing one additional unit of effort x^i to work and family matters is negligible if there already has been significant investments made on that front. Moreover, we assume that the family $\left(e^{-\int_0^t r(\omega,s)\,ds} u^i(x^i(\omega,t), C(\omega,t)),\ (x,C) \in \prod_{i=1}^n \mathscr{B}_{w^i}\right)$ is $\mathbf{P}\otimes dt$-uniformly integrable (to ensure the well-definedness of the expected utility (payoff) functions of WFH employees). The Inada conditions guarantee that there will be an interior solution for optimal effort amounts in work and family matters for any given employee. Note that since u^i is concave in c, $e^{-\int_0^t r(s)\,ds} u^i_c(x(t), C(t))$ is $\mathbf{P}\otimes dt$-integrable for any $(x,C) \in \prod_{i=1}^n \mathscr{B}_{w^i}$ such that $C(0) > 0$ a.s. Furthermore, the stochastic process ψ_c is a supermartingale (same holds for stochastic process ψ_x) and hence lower semicontinuous in expectation also from the left, i.e., $\mathbb{E}\left[\psi_c(u)\big|_t\right] \le e^{-\int_0^t r_c(s)ds}\mathbb{E}\left[\mathscr{E}_c(u)\big|_t\right] = \psi_c(t)$. Here, a stochastic process is *lower-semicontinuous in expectation* Dellacherie et al. (1978) if for any stopping time τ one has $\liminf_{n\uparrow\infty} \mathbb{E}[X(\tau_n)] \ge \mathbb{E}[X(\tau)]$, whenever $\{\tau_n\}_{n\in\mathbb{N}}$ is a monotone sequence of stopping times converging to τ.

3 THE BENCHMARK FOR EMPLOYEE-AGGREGATE EFFORT IN cybersecurity

In this section, we derive the benchmark amount of employee-aggregate investment efforts (that will also include individual employee benchmarks) that an organization would ideally want its WFH employees to put in towards ensuring cybersecurity best practices.

Throughout this section, denote by $(\underline{x}, \underline{C})$ a vector of investment processes valued in $\mathbb{R}^{2n}_+$ with components $(x^1, \dots, x^n, C^1, \dots, C^n)$ The C-Suite of given organization with n WFH employees is interested to obtain as a benchmark solution the maximized aggregate expected utility of its employees through the allocation of appropriate efforts, both in work and family matters, and in cybersecurity best practices. This amounts to solving a social planner (SP) optimization problem with value

$$V_{SP}(w) := \sup_{(\underline{x},\underline{C})\in\mathscr{B}_w} U_{SP}(\underline{x},\underline{C}) := \sup_{(\underline{x},\underline{C})\in\mathscr{B}_w} \sum_{i=1}^n \gamma^i U^i(x^i, C^i; C^{-i}) \tag{3}$$

with $U^i(x^i, C^i; C^{-i})$ as in (2) and for given positive weights γ^i, $i = 1, \dots, n$, such that $\sum_{i=1}^n \gamma^i = 1$. Throughout the rest of the paper, $(\underline{x}, \underline{C})$ is a vector of time-varying effort investment stochastic processes valued in $\mathbb{R}^{2n}_+$

with components $(x^1,\dots,x^n,C^1,\dots,C^n)$. We now have the following result stating a unique solution to the C-Suite optimization problem.

Theorem 1 *There exists a unique $(\underline{x}_*,\underline{C}_*)\in\mathscr{B}_w$ that solves the C-Suite optimization problem* (3) *and benchmarks over the period $[0,T]$ - the optimal effort pair $(\underline{x}_*,\underline{C}_*)$ that n WFH employees of an organization should ideally invest in both, work and family matters, and in cybersecurity best practices. The unique solution to $(\underline{x}_*,\underline{C}_*)$ is given by*

$$\begin{cases} C_*(t)=\sum_{i=1}^n C_*^i(t)=\sup_{0\le u\le t} l^*(u)\vee 0,\\ \\ x_*^i(t)=g^i\Big(\frac{\lambda_*}{\gamma^i}\psi_x(t),C_*(t)\Big),\ \ i=1,\dots,n, \end{cases}$$

where l^* is the unique solution of

$$\mathbb{E}\left[\int_\tau^T e^{-\int_0^t r(s)\,ds}\sum_{i=1}^n \gamma^i h^i\left(\frac{\lambda}{\gamma^i}e^{\int_0^t r(u)du}\psi_x(t),\ \sup_{\tau\le u\le t} l(u)\right)dt\ \middle|\ \mathscr{F}_\tau\right]=\lambda\,\psi_c(\tau)1_{\{\tau<T\}}$$

*for (a) any stopping time $\tau\in[0,T]$ subject to $l_T^*=0$, **P**-a.s., and (b) a suitable Lagrange multiplier $\lambda_*>0$ such that $\sum_{i=1}^n\Psi(x_*^i,C_*^i)=w$. Here, $g^i(\cdot,c)$ is the inverse of $u_x^i(\cdot,c)$, for all $i=1,\dots,n$, and $h^i(\psi,c):=u_c^i(g(\psi,c),c)$ for any $\psi,c>0$.*

Proof Sketch (in the interest of space) - Generate expectation estimates $\tilde{\mathbb{E}}_c$ and $\tilde{\mathbb{E}}_x$ under the measures $\tilde{\mathbf{P}}_c$ and $\tilde{\mathbf{P}}_x$ on $\mathscr{F}_T$ with Radon-Nikodym derivative $\mathscr{E}_c(T)$ and $\mathscr{E}_x(T)$, respectively, with respect to $\mathbf{P}$. Let $\{(\underline{x}_m,\underline{C}_m)\}_{m\in\mathbb{N}}\subset\mathscr{B}_w$ be a sequence of effort investment plans such that

$$\lim_{m\to\infty}\sum_{i=1}^n\gamma^i U^i(x_m^i,C_m^i;C_m^{-i})=V_{SP}.$$

Since the following relation holds for all i,

$$\begin{aligned} w&\ge\mathbb{E}\left[\int_0^T\psi_x(t)x_m^i(t)dt\right]=\mathbb{E}\left[\int_0^T e^{-\int_0^t r_x(s)ds}[\mathscr{E}_x(T)|_t]\,x_m^i(t)dt\right]\\ &=\mathbb{E}\left[\mathscr{E}_x(T)\int_0^T e^{-\int_0^t r_x(s)ds}x_m^i(t)dt\right]\ge K_1\tilde{\mathbb{E}}_x\left[\int_0^T x_m^i(t)dt\right], \end{aligned}$$

each $\{x_m^i\}_{m\in\mathbb{N}}$, $i=1,\dots,n$, is L^1-bounded as sequence of random variables on the probability space $(\Omega\times[0,T],\mathscr{O},d\mu_x)$, where $\mathscr{O}$ is the optional σ-algebra. Hence by Komlós' theorem (Komlós 1967), for every $i=1,\dots,n$ there exist two subsequences $\{\tilde{x}_m^i\}_{m\in\mathbb{N}}\subset\{x_m^i\}_{m\in\mathbb{N}}$ and $\{\tilde{C}_m^i\}_{m\in\mathbb{N}}\subset\{C_m^i\}_{m\in\mathbb{N}}$; a $d\mu_x$-integrable and optional process x_*^i; and some optional random measure dC_*^i, $i=1,\dots,n$, s.t., as $k\uparrow\infty$,

$$X_k^i(t):=\frac{1}{k+1}\sum_{m=0}^k\tilde{x}_m^i(t)\to x_*^i(t),\ d\mu_x\text{-a.e., and}$$

$$I_k^i(t):=\frac{1}{k+1}\sum_{m=0}^k\tilde{C}_m^i(t)\to C_*^i(t)\text{ for every point of continuity of }C_*^i(\cdot)\text{ and }t=T,\tilde{}_c\text{-a.s.}$$

Using Fatou's Lemma, we can claim that the Komlós' limit $(\underline{x}_*,\underline{C}_*):=(x_*^1,\dots,x_*^n,C_*^1,\dots,C_*^n)$ belongs to $\mathscr{B}_w$ and it is optimal for the social planner's objective function in (3). Indeed, $(\underline{X}_k,\underline{I}_k):=(X_k^1,\dots,X_k^n,I_k^1,\dots,I_k^n)\in\mathscr{B}_w$ by convexity of $\mathscr{B}_w$, and $(\underline{x}_*,\underline{C}_*)\in\mathscr{B}_w$. The uniqueness of the optimal solution $(\underline{x}_*,C_*)$ up to indistinguishability follows from strict concavity of the utility functions u^i, $i=1,\dots,n$, and from convexity of $\mathscr{B}_w$.

Implications to Organizational Cyber-Risk Management - The theorem provides the C-Suite of an organization with a unique, optimal, and closed form characterization of the amount of effort its n WFH employees should split between work-family activities and ensuring cybersecurity best practices. This benchmark information will also be of interest to cyber-insurers that individually insure employees in the WFH era through personal contracts - acting as a rough estimate of the best possible cyber-hygiene an employee could adopt, given current technology. We also observe through the theorem that (a) the optimal relative effort, $\frac{x^i_*(t)}{w}$ in work-family matters for each WFH employee n is independent of n, and (b) the contributed aggregate cybersecurity public good is proportional to n. Both (a) and (b) align with practical world, simply because employee work-family efforts are scarcely dependent on the other employees in an organization, and the quality of cybersecurity as a public good scales with a positive contribution by each WFH employee. To simply capture the essence of (a) and (b) above, consider the special case of symmetric players - each having (i) the same individual utility function in the Cobb-Douglas sense (a standard utility function in micro-economic theory), i.e., $u^i(x,c) = \frac{x^\alpha c^\beta}{\alpha+\beta}$ for all i with $\alpha+\beta \leq 1$, (ii) $\gamma^i = \frac{1}{n}$ for all i, and (iii) the per-unit effort costs being general exponential Lévy processes (that include Brownian Motion) $\psi_x(t) = e^{-rt}\mathscr{E}_x(t)$ and $\psi_c(t) = e^{-rt}\mathscr{E}_c(t)$. We get the optimal effort characterization satisfying (a) and (b) as given by $C_*(t) = l_0\theta(t)$; $x^i_*(t) = \frac{1}{n}l_0\gamma(t), \forall i$; and $\lambda_* = \frac{1}{n^\alpha}A^{1-\alpha}l_0^{\alpha+\beta-1}$, where $\theta(t) := \sup_{0\leq s\leq t}\left(\mathscr{E}_c^{-\frac{1-\alpha}{1-\alpha-\beta}}(s)\mathscr{E}_x^{-\frac{\alpha}{1-\alpha-\beta}}(s)\right)$, $\gamma(t) := \frac{1}{A}\left[\left(\frac{\alpha+\beta}{\alpha}\right)\mathscr{E}_x(t)\inf_{0\leq s\leq t}\left(\mathscr{E}_c^{\frac{\beta(1-\alpha)}{1-\alpha-\beta}}(s)\mathscr{E}_x^{\frac{\alpha\beta}{1-\alpha-\beta}}(s)\right)\right]^{-\frac{1}{1-\alpha}}$, $l_0 := \frac{n\cdot w|w=w^i,\forall i}{\mathbb{E}\left[\int_0^T \psi_x(t)\gamma(t)dt + \int_0^T \psi_c(t)d\theta(t)\right]}$, $A := \mathbb{E}\left[\int_0^T \delta e^{-ru}\inf_{0\leq s\leq u}\left(\mathscr{E}_c(s)\mathscr{E}_x^{-\frac{\alpha}{1-\alpha}}(u-s)\right)du\right]$, and $\delta := \frac{\beta}{\alpha}\left(\frac{\alpha+\beta}{\alpha}\right)^{\frac{1}{\alpha-1}}$. Conditions (a) and (b) hold.

4 HOW MUCH DO STRATEGIC WFH EMPLOYEES INVEST IN cybersecurity?

In this section, we focus on the practically realistic situation where WFH employees work in 'non'-controlled distributed home "siloes". Here, the term 'non'-controlled implies either a zero or partial control of the IT managerial team on the cybersecurity practices of individual WFH employees . The employees are assumed to have free-will to manage their cyber-hygiene, as is usual in practice. We derive the strategic amount of employee-aggregate investment efforts (includes individual effort) at a strategic equilibrium (conditioned on its existence), when compared to the benchmark amount in Section 3.

We consider a game-theoretic setting where each WFH employee i's optimal choice of a strategy, i.e., it's investment towards the cybersecurity public good, against a given stochastic process C^{-i} specifying aggregate contributions by the 'opponent' WFH employees is equivalent to solving the stochastic control problem with value function

$$V^i(C^{-i}) := \sup_{(x^i,C^i)\in\mathscr{B}_{w^i}} U^i(x^i,C^i;C^{-i}), \qquad i=1,\ldots,n,$$

where $\mathscr{B}_{w^i}$ and U^i are as in (1) and (2), respectively. A Nash equilibrium of this game is a tuple $(\hat{x}^1,\ldots,\hat{x}^n,\hat{C}^1,\ldots,\hat{C}^n)$ that for all $i\in\{1,\ldots,n\}$, satisfies $(\hat{x}^i,\hat{C}^i)\in\mathscr{B}_{w^i}$ and $U^i(\hat{x}^i,\hat{C}^i;\hat{C}^{-i}) = V^i(\hat{C}^{-i})$. The concept of the Nash equilibrium just proposed does limit the WFH employees to react to the evolving exogenous uncertainty - specifically, they assume as given the effort contribution processes of peer WFH employees as given and do not react to deviations from announced (equilibrium) play. There are significant practical challenges to define a strategic solution concept incorporating explicit feedback challenges (Back and Paulsen 2009). Hence, we stick with a simple open-loop Nash equilibrium to account for the case when the WFH employees are not able to observe others' effort actions. We have the following result regarding the Nash equilibrium of the WFH efforts investment game.

Theorem 2 *Let $x^i \in \mathbb{L}^2(d\mu_x)$ for all $i=1,\ldots,n$. There exists a pure-strategy Nash equilibrium $(\hat{x}^i,\hat{C}^i)_{i\in 1,\ldots,n} \in \Pi_{i=1}^n\mathscr{B}_{w^i}$ of efforts towards work-family matters and cybersecurity best practices for the WFH efforts in-*

vestment game that satisfies:

$$U^i(\hat{x}^i,\hat{C}^i;\hat{C}^{-i}) \geq U^i(x^i,C^i;\hat{C}^{-i}), \forall (x^i,C^i) \in \mathscr{B}_{w^i}, x^i \in \mathbb{L}^2(d\mu_x), i=1,\ldots,n,$$

where $\mathbb{L}^2$ is the space of square integrable functions with respect to $d\mu_x = d\tilde{\boldsymbol{P}}_x \otimes dt$.

Proof Sketch (in the interest of space) - In order to prove the existence of a pure strategy Nash equilibrium of the investment efforts game, we will combine arguments from conjugate duality theory and the general theory of stochastic processes to apply the *Kakutani-Fan-Glicksberg Theorem* (Maschler et al. 2013) that proves the existence of a pure strategy Nash equilibrium. To start with, an application of the *Girsanov Theorem* Dellacherie et al. (1978) with the fact that $x^i \in \mathbb{L}^2(d\mu_x)$, $i=1,\ldots,n$, implies that x^i incurs a finite budget at any time instant. The steps to show the existence of a Nash equilibrium will necessitate applying some fixed point argument, and hence to proving compactness of the set of admissible strategies and continuity (or even upper semicontinuity) of the payoff functionals. By employing a duality approach, we will first prove that set $\mathscr{K}_{w^i}$ is a compact subset of $\mathbb{L}^2(d\mu_x)$ with respect to the weak-topology $\sigma(\mathbb{L}^2(d\mu_x),\mathbb{L}^2(d\mu_x)$. Likewise, we will then prove that set $\mathscr{S}_{w^i}$ is a compact subset with respect to a weak-topology. Subsequently, we will prove the set $\mathscr{A}_{w^i}$ is a compact subset with respect to a weak-topology. In order to prove the above three compactness results, we use the *Banach-Alaoglu Theorem* Aliprantis and Border (1994). We will then show that the mapping $(x^i,C^i) \mapsto U^i(x^i,C^i;C^{-i})$ is upper semi-continuous for the weak topology $\sigma(\mathbb{L}^2(d\mu_x),\mathbb{L}^2(d\mu_x)$ using the *Banach-Saks* theorem (Bendová et al. 2015). Finally, everything falls in place to apply the Kakutani-Fan-Glicksberg Theorem to guarantee the existence of a Nash equilibrium. Here, set $\mathscr{S}_{w^i}$ is defined as $\mathscr{S}_{w^i} := \left\{ C^i : \Omega \times [0,T] \mapsto \mathbb{R}_+ \text{ optional, s.t. } C \text{ right-continuous, decreasing; } \mathbb{E}\left[\int_0^T \psi_c(t) C^i(t) dt\right] \leq w^i \right\}$; set $\mathscr{K}_{w^i}$ is defined as $\mathscr{K}_{w^i} := \left\{ x^i : \Omega \times [0,T] \mapsto \mathbb{R}_+ \text{ optional, s.t. } \mathbb{E}\left[\int_0^T \psi_x(t) x^i(t) dt\right] \leq w^i \right\}$; and set $\mathscr{A}_{w^i}$ is defined as $\mathscr{A}_{w^i} := \left\{ (x^i,C^i) : \Omega \times [0,T] \mapsto \mathbb{R}_+^2 \text{ optional}; \mathbb{E}\left[\int_0^T \psi_x(t) x^i(t) dt\right] + \mathbb{E}\left[\int_0^T \psi_c(t) C^i(t) dt\right] \leq w^i \right\}$.

Implications to Organizational Cyber-Risk Management - The theorem guarantees the existence of a pure-strategy strategic stable point in an efforts game played by free-willed WFH employees in a distributed setting, where no employee has any incentive to change its effort contributions. However, the theorem does not guarantee the existence of a unique pure-strategy Nash equilibrium - evident from the strategic substitutes nature of the security public good. From the organizational C-Suite viewpoint, this implies that perfectly rational and strategic employee behavior towards ensuring cybersecurity best practices can result in more than one stable security posture for the entire organization. The upper level management in consultation with the CIOs/CISOs should develop internal policies (e.g., employee behavior shaping programs) to ensure that the the gap between the quality of organizational security posture induced by multiple Nash equilibria is not significant (e.g., one equilibrium might result in a major ransomware attack on the organization, while the others may make the organization susceptible to minor cyber-threats). To intuitively capture the essence of the existence of the pure-strategy Nash equilibrium above, consider the special case of symmetric players - each having (i) the same individual utility function in the Cobb-Douglas sense (a standard utility function in micro-economic theory), i.e., $u^i(x,c) = \frac{x^\alpha c^\beta}{\alpha+\beta}$ for all i with $\alpha+\beta \leq 1$, (ii) $\gamma^i = \frac{1}{n}$ (each WFH employee's payoff contributing equally to net organizational value) and $w^i = w$ (equal budget for every WFH employee) for all i, and (iii) the per-unit effort costs being general exponential Lévy processes (that include Brownian Motion) $\psi_x(t) = e^{-rt}\mathscr{E}_x(t)$ and $\psi_c(t) = e^{-rt}\mathscr{E}_c(t)$. The Nash equilibrium of the efforts investment game is given by $\hat{C}_*(t) = \frac{\kappa}{n}\theta(t)$; $\hat{x}^i_*(t) = \kappa\gamma(t), \forall i$; and $\lambda^i = A^{1-\alpha}\kappa^{\alpha+\beta-1}, \forall i$, where $\theta(t) := \sup_{0\leq s\leq t}\left(\mathscr{E}_c^{-\frac{1-\alpha}{1-\alpha-\beta}}(s)\mathscr{E}_x^{-\frac{\alpha}{1-\alpha-\beta}}(s)\right)$, $\gamma(t) := \frac{1}{A}\left[\left(\frac{\alpha+\beta}{\alpha}\right)\mathscr{E}_x(t)\inf_{0\leq s\leq t}\left(\mathscr{E}_c^{\frac{\beta(1-\alpha)}{1-\alpha-\beta}}(s)\mathscr{E}_x^{\frac{\alpha\beta}{1-\alpha-\beta}}(s)\right)\right]^{-\frac{1}{1-\alpha}}$, $\kappa := \frac{w}{\mathbb{E}\left[\int_0^T \psi_x(t)\gamma(t)dt + \frac{1}{n}\int_0^T \psi_c(t)d\theta(t)\right]}$, $A :=$

$\mathbb{E}\left[\int_0^T \delta e^{-ru} \inf_{0\le s\le u}\left(\mathscr{E}_c(s)\mathscr{E}_x^{-\frac{\alpha}{1-\alpha}}(u-s)\right)du\right]$, and $\delta := \frac{\beta}{\alpha}\left(\frac{\alpha+\beta}{\alpha}\right)^{\frac{1}{\alpha-1}}$. We also observe through the simple symmetric case example (similar to that in Theorem 1) that (a) the optimal relative effort, $\frac{x_*^i(t)}{w}$ in work-family matters for each WFH employee n is independent of n, and (b) the contributed aggregate cybersecurity public good is proportional to n. Both (a) and (b) align with practical world, simply because employee work-family efforts are usually scarcely dependent (if at all) on the other employees in an organization, and the quality of cybersecurity as a public good scales with a positive contribution by each WFH employee. However, in strange contrast to a centralized control regime, the individual contributions to the security public good is independent (scarcely dependent at best) of n - the number of WFH employees. This is because the positive externality contributed by each symmetric WFH employee through their efforts in cybersecurity best practices cancels out in a symmetric setting. This will not be the case in realistic asymmetric WFH settings, where $\hat{C}_*(t)$ will depend on the γ^i values and n.

5 HOW MUCH IS THE DEGREE OF SUBOPTIMAL cybersecurity (FREE-RIDING)?

In this section, we quantify the dynamic degree (over time) of sub-optimality in the cybersecurity incurred by an organization working in WFH mode.

The dynamic degree of sub-optimality in the cybersecurity strength of an organization can be captured using the free-riding measure – in our case, the time-varying ratios of the benchmark optimal employee-aggregate efforts towards ensuring cybersecurity best practices, and the strategic Nash equilibrium (distributed optimal) of similar employee-aggregate efforts. We have the following result stating the degree of of sub-optimal cybersecurity an organization with n WFH employees incur.

Theorem 3 *The degree of sub-optimality in the cybersecurity strength incurred by an organization with n WFH employees is given by*

$$\frac{C_*(t)}{\hat{C}(t)} = \frac{l_0}{\kappa} = \frac{\mathbb{E}\left[n\int_0^T e^{-rt}\mathscr{E}_x(t)\gamma(t)dt + r\int_0^T e^{-rt}\theta(t)dt\right]}{\mathbb{E}\left[\int_0^T e^{-rt}\mathscr{E}_x(t)\gamma(t)dt + r\int_0^T e^{-rt}\theta(t)dt\right]} \ge 1,$$

where $\frac{C_*(t)}{\hat{C}(t)}$ is often termed as the extent of free-riding with respect to a public good (in our case, WFH employee effort in ensuring cybersecurity best practices). Moreover, in the special case of symmetric WFH employees, the sub-optimality can be tightly bounded through by the following closed form expression. $\frac{C_*(t)}{\hat{C}} = \frac{n\alpha+\beta}{\alpha+\beta} \ge 1$, where each WFH employee has a Cobb-Douglas utility function of the form $u^i(x,c) = \frac{x^\alpha c^\beta}{\alpha+\beta}$ for all i with $\alpha+\beta \le 1$, $\gamma^i = \frac{1}{n}$ for all i, and the per-unit effort costs being general exponential Lévy processes (that include Brownian Motion) $\psi_x(t) = e^{-rt}\mathscr{E}_x(t)$ and $\psi_c(t) = e^{-rt}\mathscr{E}_c(t)$.

Proof Sketch (in the interest of space) - The first part of the theorem is easily follows from $C_*(t)$ and $\hat{C}_*(t)$ expressions in Theorems 1 and 2 respectively. In order to show the second part involving the special case of symmetric WFH work environments, recall γ from Theorems 1 and 2, and use a fact from excursion theory for Lévy processes that $W(t) - \sup_{0\le u\le t} W(u)$ is independent of $\sup_{0\le u\le t} W(u)$, and a fact from the *Duality Theorem* Dellacherie et al. (1978) that says that $W(t) - \sup_{0\le u\le t} W(u)$ has the same distribution as $\inf_{0\le u\le t} W(u)$. Subsequent algebraic manipulations yield the desired result.

Implications to Organizational Cyber-Risk Management - The theorem provides a closed-form expression for the time-dependent ratio of the quality of the best possible cybersecurity posture achievable by an organization functioning in WFH mode, and the quality that is achieved in practice by perfectly rational free-willed WFH employees in a strategic Nash equilibrium. The higher the ratio, greater the sub-optimality, and we expect the ratio to be higher when WFH individuals are boundedly rational (a subject of study as part of future work). This information regarding the degree of cybersecurity sub-optimality will be of interest to cyber-insurers that individually insure employees in the WFH era through personal contracts - acting as a

rough measure of cyber-insurance market inefficiency, given current technology. This time-dependent ratio will also enable a close cooperation between these cyber-insurers and the insurers insuring cyber-losses of the organization (they could be the same entities) to design employee-centric policies that shape voluntary cyber-hygiene improving behavior of WFH employees in a manner to reduce the sub-optimality ratio.

6 SUMMARY

We proposed a novel asymmetric strategic theory to dynamically quantify the amount of free riding in cybersecurity by the employees of an organization, all of whom work in heterogeneous WFH "siloes". This is not only the first effort of its kind in the field of WFH cybersecurity, but is also, to the best of our knowledge, the first to rigorously quantify cybersecurity free-riding in heterogeneous, time-dynamic, and environment-dynamic settings. In order to achieve our goal, we first assumed the individual employee investment in cybersecurity improving efforts and their per unit cost to be time-discounted exponential martingales over time, and derived the centrally-controlled socially optimal aggregate employee effort at any given time instant. We then derived the time-varying strategic Nash equilibrium amount of aggregate employee effort in cybersecurity in a distributed setting. The time-dependent ratio of the centralized and distributed aggregate effort estimates quantified the free riding dynamics within an organization.

ACKNOWLEDGMENTS

R. Pal and R. Sequeira are the lead authors. Parts of our proof sketch for Theorem 1 are adopted and reproduced (for the purpose of consistency and self-sufficiency) from certain pieces of analytic public good economic methodologies proposed in (Varian 1994; Ferrari et al. 2017).

REFERENCES

Aliprantis, C. D., and K. C. Border. 1994. *Infinite Dimensional Analysis*. Berlin: Springer-Verlag.

Amin, S., G. A. Schwartz, and S. S. Sastry. 2011. "On the Interdependence of Reliability and Security in Networked Control Systems". In *50th IEEE Conference on Decision and Control and European Control Conference, December 12th-15th*, 4078–4083. Orlando, Florida: Institute of Electrical and Electronics Engineers, Inc.

Amin, S., G. A. Schwartz, and S. S. Sastry. 2013. "Security of Interdependent and Identical Networked Control Systems". *Automatica* 49(1):186–192.

Back, K., and D. Paulsen. 2009. "Open-Loop Equilibria and Perfect Competition in Option Exercise Games". *The Review of Financial Studies* 22(11):4531–4552.

Bag, P. K., and S. Roy. 2011. "On Sequential and Simultaneous Contributions under Incomplete Information". *International Journal of Game Theory* 40(1):119–145.

Bendová, H., O. F. Kalenda, and J. Spurnỳ. 2015. "Quantification of the Banach–Saks property". *Journal of Functional Analysis* 268(7):1733–1754.

Bergstrom, T., L. Blume, and H. Varian. 1986. "On the Private Provision of Public Goods". *Journal of Public Economics* 29(1):25–49.

Dellacherie, Claude, Meyer, and Paul-André. 1978. *Probabilities and Potential, vol. 29 of North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam.

Ferrari, G., F. Riedel, and J.-H. Steg. 2017. "Continuous-Time Public Good Contribution Under Uncertainty: A Stochastic Control Approach". *Applied Mathematics & Optimization* 75(3):429–470.

Fershtman, C., and S. Nitzan. 1991. "Dynamic Voluntary Provision of Public Goods". *European Economic Review* 35(5):1057–1067.

Gordon, L. A., M. P. Loeb, and W. Lucyshyn. 2003. "Sharing Information on Computer Systems Security: An Economic Analysis". *Journal of Accounting and Public Policy* 22(6):461–485.

Grossklags, J., N. Christin, and J. Chuang. 2008. "Secure or Insure? A Game-Theoretic Analysis of Information Security Games". In *Proceedings of the 17th international conference on World Wide Web*, 209–218. New York, NY, USA: Association for Computing Machinery.

Grossklags, J., S. Radosavac, A. A. Cárdenas, and J. Chuang. 2010. "Nudge: Intermediaries' Role in Interdependent Network Security". In *International Conference on Trust and Trustworthy Computing*, 323–336. Berlin, Heidelberg: Springer.

Groves, T., and J. Ledyard. 1977. "Optimal Allocation of Public Goods: A Solution to the "Free Rider" Problem". *Econometrica: Journal of the Econometric Society*:783–809.

Hota, A. R., and S. Sundaram. 2016. "Interdependent Security Games on Networks under Behavioral Probability Weighting". *IEEE Transactions on Control of Network Systems* 5(1):262–273.

Jiang, L., V. Anantharam, and J. Walrand. 2010. "How Bad Are Selfish Investments in Network Security?". *IEEE/ACM Transactions on Networking* 19(2):549–560.

Komlós, J. 1967. "A Generalization of a Problem of Steinhaus". *Acta Mathematica Academiae Scientiarum Hungaricae* 18(1-2):217–229.

Kunreuther, H., and G. Heal. 2003. "Interdependent Security". *Journal of Risk and Uncertainty* 26(2):231–249.

La, R. J. 2016. "Interdependent Security With Strategic Agents and Cascades of Infection". *IEEE/ACM Transactions on Networking* 24(3):1378–1391.

La, R. J. 2017. "Effects of Degree Correlations in Interdependent Security: Good or Bad?". *IEEE/ACM Transactions on Networking* 25(4):2484–2497.

Laszka, A., M. Felegyhazi, and L. Buttyan. 2014. "A Survey of Interdependent Information Security Games". *ACM Computing Surveys (CSUR)* 47(2):1–38.

Lelarge, M., and J. Bolot. 2008. "A Local Mean Field Analysis of Security Investments in Networks". In *Proceedings of the 3rd International workshop on Economics of networked systems*, 25–30. New York, NY, USA: Association for Computing Machinery.

Levhari, D., and L. J. Mirman. 1980. "The Great Fish War: An Example Using a Dynamic Cournot-Nash Solution". *The Bell Journal of Economics*:322–334.

Marx, L. M., and S. A. Matthews. 2000. "Dynamic Voluntary Contribution to a Public Project". *The Review of Economic Studies* 67(2):327–358.

Maschler, M., E. Solan, and S. Zamir. 2013. *Game Theory*. Cambridge: Cambridge University Press.

Ögüt, H., N. Menon, and S. Raghunathan. 2005. "Cyber Insurance and IT Security Investment: Impact of Interdependence Risk". In *4th Workshop on the Economics of Information Security (WEIS), June 2nd-3rd*. Cambridge, MA, USA: Information Security Economics.

Olson, M. 1965. *The Logic of Collective Action*. Cambridge, Mass.: Harvard Univ. Press.

Pal, R., and L. Golubchik. 2010. "Analyzing Self-Defense Investments in Internet Security under Cyber-Insurance Coverage". In *Proceedings of 2010 IEEE 30th International Conference on Distributed Computing Systems*, 339–347. Los Alamitos, CA, USA: Institute of Electrical and Electronics Engineers, Inc.

Pal, R., and P. Hui. 2011. "Modeling Internet Security Investments: Tackling Topological Information Uncertainty". In *International Conference on Decision and Game Theory for Security*, 239–257. Berlin, Heidelberg: Springer.

Palfrey, T. R., and H. Rosenthal. 1984. "Participation and The Provision of Discrete Public Goods: A Strategic Analysis". *Journal of Public Economics* 24(2):171–193.

Samuelson, P. A. 1954. "The Pure Theory of Public Expenditure". *The Review of Economics and Statistics* 36(4):387–389.

Takayama, A., and T. Akira. 1985. *Mathematical Economics*. Cambridge: Cambridge University Press.

Varian, H. 2004. "System Reliability and Free Riding". In *Economics of Information Security*, 1–15. Springer.

Varian, H. R. 1994. "Sequential Contributions to Public Goods". *Journal of Public Economics* 53(2):165–186.

Wang, W. K., and C. O. Ewald. 2010. "Dynamic Voluntary Provision of Public Goods with Uncertainty: A Stochastic Differential Game Model". *Decisions in Economics and Finance* 33(2):97–116.

Yeung, D. W., and L. A. Petrosyan. 2013. "Subgame Consistent Cooperative Provision of Public Goods". *Dynamic Games and Applications* 3(3):419–442.

AUTHOR BIOGRAPHIES

RANJAN PAL is a researcher with the Cambridge Trust and Technology Initiative at the University of Cambridge, UK. His primary research interest lies in engineering cyber-risk management solutions using economics, decision science, and the applied mathematical sciences. He is a member of the IEEE and the ACM, and serves as an Associate Editor of the ACM Transactions on MIS. His emil address is the.gallivant.theorist@gmail.com.

ROHAN XAVIER SEQUEIRA is a graduate student and a graduate student instructor in Electrical and Computer Engineering at the University of Michigan, USA. His research interest lies is cyber-risk management and computer networks. He is a student member of the IEEE. His email address is rohseque@umich.edu.

YUFEI ZHU is a graduate student in Computer Engineering at the University of Michigan, USA. Her research interest is cyber-risk management. She is a student member of the IEEE. Her email address is louiszyf@umich.edu.

YUSHI SHE is an undergraduate student in Computer Science at the University of Michigan, USA. His research interests lie in cyber-risk management and AI. He is a student member of the IEEE. His email address is andrsh@umich.edu.