Games and Economic Behavior 105 (2017) 230–254

Contents lists available at ScienceDirect

Games and Economic Behavior

www.elsevier.com/locate/geb

# Contagion exposure and protection technology

Diego A. Cerdeiro [1]

*International Monetary Fund, United States*

ARTICLE INFO

*Article history:*
Received 20 March 2016
Available online 2 August 2017

*JEL classification:*
C72
D62

*Keywords:*
Contagion
Protection
Exposure
Degree distribution
Technology adoption
Epidemics

ABSTRACT

Individuals adopt diverse measures to prevent contagion during interactions. I propose a model to study the implications of the protection technology on the prevalence of infections and on welfare at different levels of exposure. I find that the effect of aggregate exposure on prevalence and on protection inefficiencies depends crucially on the characteristics of the available protection technology. For example, a vaccine may yield lower infection rates and smaller costs of decentralization as exposure increases, but only if the protection it provides is sufficiently long lasting. Other protection technologies, such as those used for cybersecurity, may lead to coordination failures. The analysis has implications for disease eradication, the desirability of interventions with and without universal vaccines, and coordination failures in cybersecurity.



## 1. Introduction

The fears of pandemic raised by the 2014 Ebola outbreak were a crude reminder of the undesired side-effects of the agglomeration of human population that took place over the last centuries.[2] As highlighted by Jackson et al. (2015a), social distances have decreased dramatically in modern times, and "[t]he combination of world population growth and an increasingly interconnected society is producing new dynamics." Indeed, the potential propagation of infectious diseases due to greater exposure to contagion will almost certainly continue to be a challenge in the future, as the fraction of the population living in cities is projected to increase from 77% in 2011 to 86% in 2050 in developed countries, and from 47% to 64% in developing countries (United Nations, 2012). As economies become increasingly reliant on digital networks, concerns about contagion (of various types of malware) also extend to cybersecurity, with firms and countries shoring up their defenses.[3] The general prospect of increasing exposure in physical and online environments raises both positive and normative

*E-mail address:* dcerdeiro@imf.org.

[1] This paper is based on a chapter of my dissertation at the University of Cambridge. I am very grateful to Sanjeev Goyal for invaluable guidance and constant support, and to Marcin Dziubiński, Andrea Galeotti, and Edoardo Gallo for very detailed comments on an earlier draft. The suggestions by an Advisory Editor and two anonymous referees have greatly improved the paper. I am also grateful to Vessela Daskalova, David Easley, Julien Gagnon, Matt Leister, Francesco Nava, Anja Prummer and Flavio Toxvaerd for very helpful discussions. All remaining errors are my own. Financial support from Queens' College, Cambridge and the Cambridge Overseas Trust is gratefully acknowledged.

[2] The bubonic plague repeatedly decimated London's population in the 16th and 17th centuries (see e.g. Sutherland, 1972 and Appleby, 1980). The Spanish influenza epidemic of 1918–1920, with an estimated global toll of 50 million lives, featured higher death rates in more densely populated areas (Johnson and Mueller, 2002; Chandra et al., 2013). High population density contributed to the rapid spread of the 2009 influenza pandemic in Mexico, where the pandemic originated (Zepeda-Lopez et al., 2010).

[3] Global information-security spending was projected at $79.9 billion for 2015, and expected to reach $101 billion by 2018 ("Cyberdefense Spending Rises Amid High-Profile Hacks," *Wall Street Journal*, April 8, 2015). Ensuring a smooth functioning of digital networks has also become a primary concern for policy makers in several countries. In the US, the 2012–2016 Infrastructure Protection Strategic Plan states that "Our Nation's critical infrastructure – both

http://dx.doi.org/10.1016/j.geb.2017.07.007
0899-8256/

questions. Should we expect more intense exposures to inevitably lead to higher prevalence of infections? To what extent are policy interventions desirable?

Changes in exposure associated with an increasingly interconnected society may be beyond the control of the individual, and inquiring into its consequences is thus seemingly beyond the scope of economic theory. Yet, people, firms and countries actively protect against the threat of contagion using a variety of measures, and the study of strategic protection choices falls into a long tradition in economics examining the incentives for technology adoption that goes back to at least Griliches (1957). This paper contributes to the economics literature on contagion by showing how the relation between the strategic adoption of protection and aggregate exposure crucially depends on the characteristics of the relevant protection technology.

I consider a tractable extension of the susceptible-infected-susceptible (SIS) model that incorporates strategic protection decisions under various possible technologies.[4] The novel classification of protection technologies that I propose is based on the observation that, while investments in protection typically depreciate, when and how they do so very much depends on the context.

In many cases the protection technology is essentially interaction-specific. These include, for example, the use of hand sanitizer or a face mask, or avoiding social encounters. The cost of protection against contagion in these cases must be borne during each interaction. Alternatively, some technologies have the form of a fixed cost that, once paid, allows the individual to enjoy the benefits of protection in multiple interactions. Vaccination, which provides protection over multiple encounters but ceases to be effective if the disease mutates, is a canonical example.

In the context of cybersecurity, while protection partly involves variable costs that scale up with exposure and entails some fixed updating costs (e.g. anti-virus softwares take up processing power and require updates), a unique feature of cyber-defenses is the non-trivial costs of rebuilding after infection. For individuals, restoring protection after a security breach involves tasks ranging from re-installation of antivirus software, to changing passwords or resetting all credentials (with all these tasks being dictated by the breach and not because of a regular update). For firms and other institutions, this usually entails major outlays, over and above any losses associated with the breach per se (lost revenues, or brand damage, etc.), usually requiring e.g. the temporary hiring of dedicated experts.[5]

Motivated by these examples, I consider a classification that distinguishes between two 'pure' types of technologies. On the one hand, investments in protection whose expiration takes place *exogenously*, with an exogenously given per-period probability. Parameterized by this probability we encompass a wide spectrum of protective measures, ranging from interaction-specific protection to vaccines that never expire (so-called 'universal vaccines'). On the other hand, I consider the implications of protection investments that fully depreciate (i.e. expire) upon infection. As the probability of infection is affected by others' investment in protection, in this case the expiration of protection is essentially *endogenous*.

I find that inefficiencies associated with decentralized protection decisions, and thus the desirability of interventions, critically depend on the characteristics of the available protection technology. Individual incentives to protect under exogenous expiration will increase hand in hand with exposure only if expiration takes place with low enough probability. The first main result of the paper (Theorem 1) shows that there exists a unique threshold for the durability of protection such that if durability is below, low-degree individuals find protection most attractive.[6] Since meetings are relatively rare, a one-off payment for protection buys low-degree individuals a relatively long (expected) stream of health premium. Together with the fact that investments in protection are substitutes, the implication is that the desirability of interventions will generally be non-monotonic in population density. The intuition is as follows. Because protection decisions are substitutes, when population density is low so that prevalence is low even without protection, individuals will (inefficiently) not protect in equilibrium. At the other end, if population density is high, there will be reasons not to protect because protection is expensive. In between there will generally be some level of protection. While the prevalence of infections increases monotonically with population density, decentralization costs will be higher for societies that are either relatively sparse or very dense.

Individual incentives, and thus aggregate results, are tipped over if the durability of protection is on the other side of the threshold. In particular, results become a mirror image of the ones just described: with durable protection, it is the

physical and cyber – is crucial to the functioning of the American economy and our way of life. [...] Our critical infrastructure is increasingly connected and interdependent and protecting it and enhancing its resilience is an economic and national security imperative" (Department of Homeland Security, 2012).

[4] For an introduction to the SIS model, see e.g. Anderson and May (1992).

[5] In a recent survey of more than five thousand companies distributed over 26 countries, the average cost of a security breach has been found to be of about half a million U.S. dollars, with 69% of respondents indicating the need to hire IT consultants to restore security (Kaspersky Lab, 2016). British telecommunications firm TalkTalk, for example, hired defense company BAE Systems to restore system integrity after their 2015 high-profile cyber-attack. While details of the contract are not publicly available, exceptional expenses related to the cyber-attack (which are distinct from the loss of customers, and thus revenues, due to brand damage) amounted to GBP 39 mn or 103% of operating profits (TalkTalk Group, 2016, p. 82). After their 2014 cyber-attack, Sony hired security company Mandiant, with costs related to "investigation and remediation activities" amounting to Y$4.9 bn or 12% of net income before taxes (Sony Corporation, 2015). These costs do not include, inter alia, reputational damage or payments related to class action suits by firm employees whose personal data were stolen. The company's filings flag cyber-attacks as one of the major risks to its operations, indicating that "[...] a breach of a business partner's information security may result in unauthorized access to Sony's business information, including proprietary information, intellectual property, employee information and data related to Sony's customers, suppliers and other business partners."

For further details on these cyber-attacks, see e.g. "TalkTalk cyber attack: what we know about the hack," (*Financial Times*, October 23, 2015), and "Behind the Scenes at Sony as Hacking Crisis Unfolded," (*The Wall Street Journal*, December 30, 2014).

[6] Following several papers in the literature, I will denote the level of exposure to interactions as *degree*, and refer to exposure and degree interchangeably. I will use 'population density' when referring to the average degree in the population.