Online Promiscuity

Prophylactic Patching and the Spread of Computer Transmitted Infections

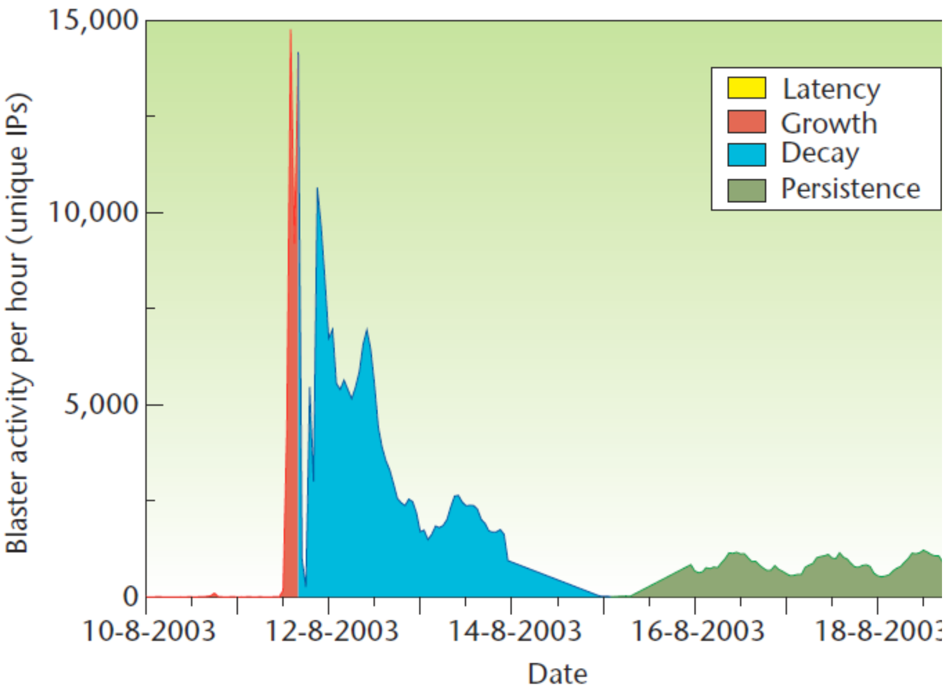
Timothy Kelley and L. Jean Camp
Indiana University Bloomington
School of Informatics and Computing

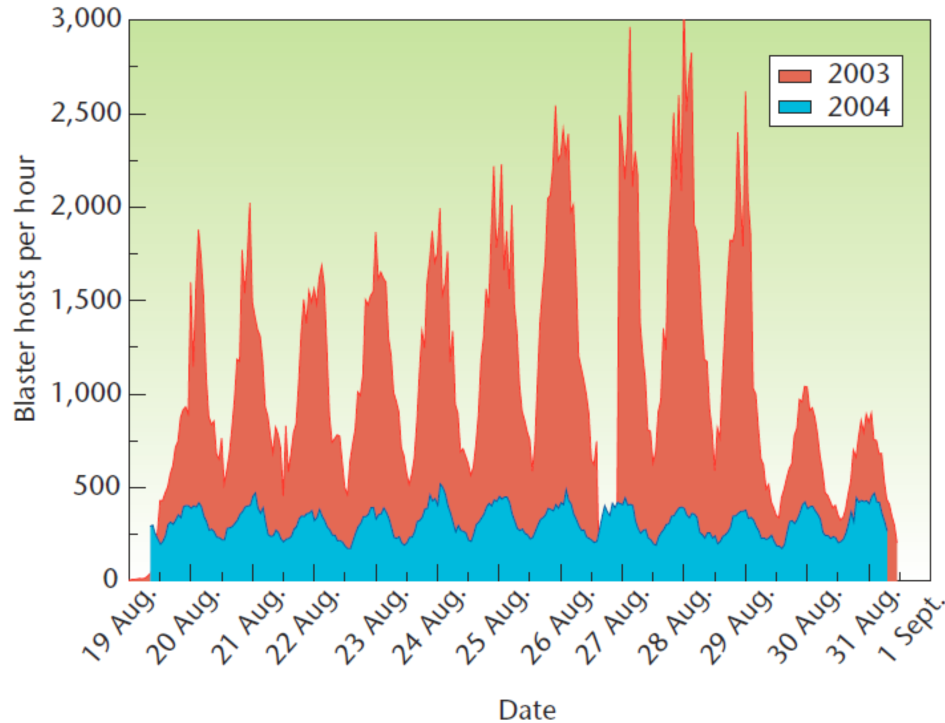
The first author acknowledges VolkswagenStiftung for a travel grant to attend WEIS 2012 in Berlin.

Research Questions

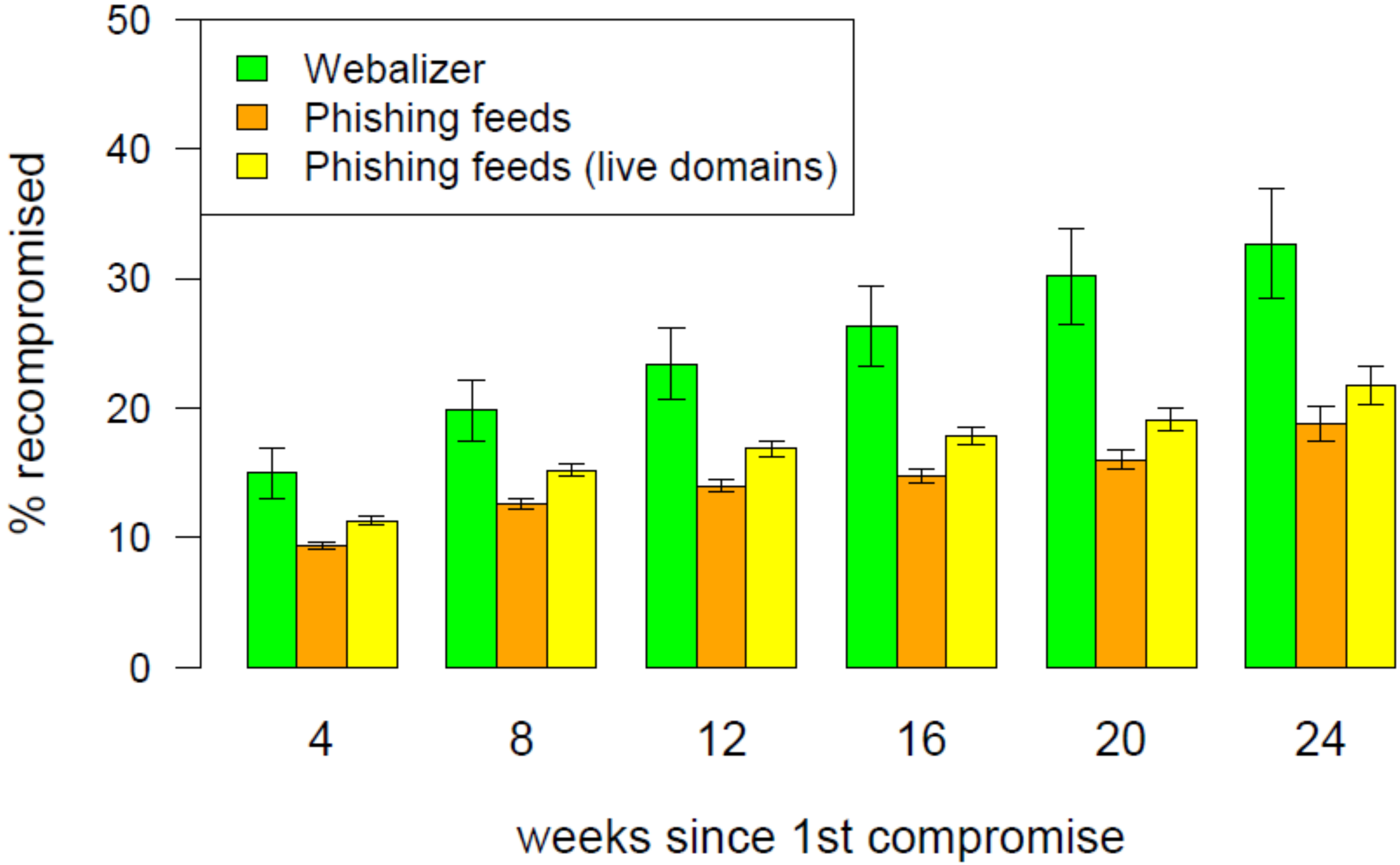
- How can exploratory epidemiological models help us better quantify online risk?
  - How can we use exploratory epidemiological models to help us better understand the risks due to online risk takers?

Motivation and Related Work



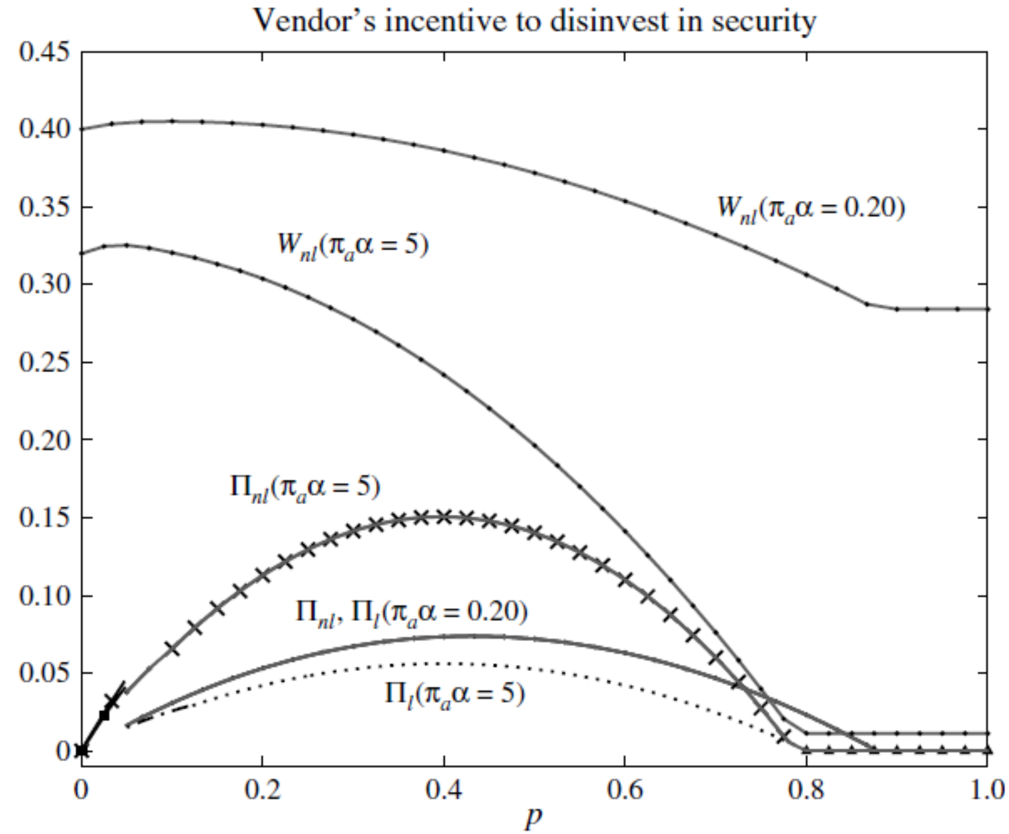


Bailey, M., Cooke, E., Jahanian, F., Watson, D., & Nazario, J. (2005). The Blaster Worm: Then and Now. *IEEE Security and Privacy Magazine*, *3*(4), 26-31. doi: 10.1109/MSP.2005.106



Moore, T., & Clayton, R. (2009). Evil searching: Compromise and recompromise of internet hosts for phishing. *Financial Cryptography and Data Security*, 256-272. Barbados. Retrieved from http://www.springerlink.com/index/0W7832116242 3252.pdf

Figure 4 **Security Risk Used as a Strategic Tool by a Profit-Maximizing Vendor Who Enforces Security Patch Restrictions**



Notes. Profit and welfare curves are illustrated for low effective security risk ($\pi_a\alpha = 0.20$) and high effective security risk ($\pi_a\alpha = 5$) under both nonrestrictive ($\rho = l$) and restrictive ($\rho = nl$) security patch policies. The remaining parameters are $c_p = 0.20$, $\pi_d c_d = 0.05$, and $\nu = 0.65$.

August, T., & Tunca, T. I. (2008). Let the Pirates Patch? An Economic Analysis of Software Security Patch Restrictions. *Information Systems Research*, *19*(1), 48-70. doi:10.1287/isre.1070.0142

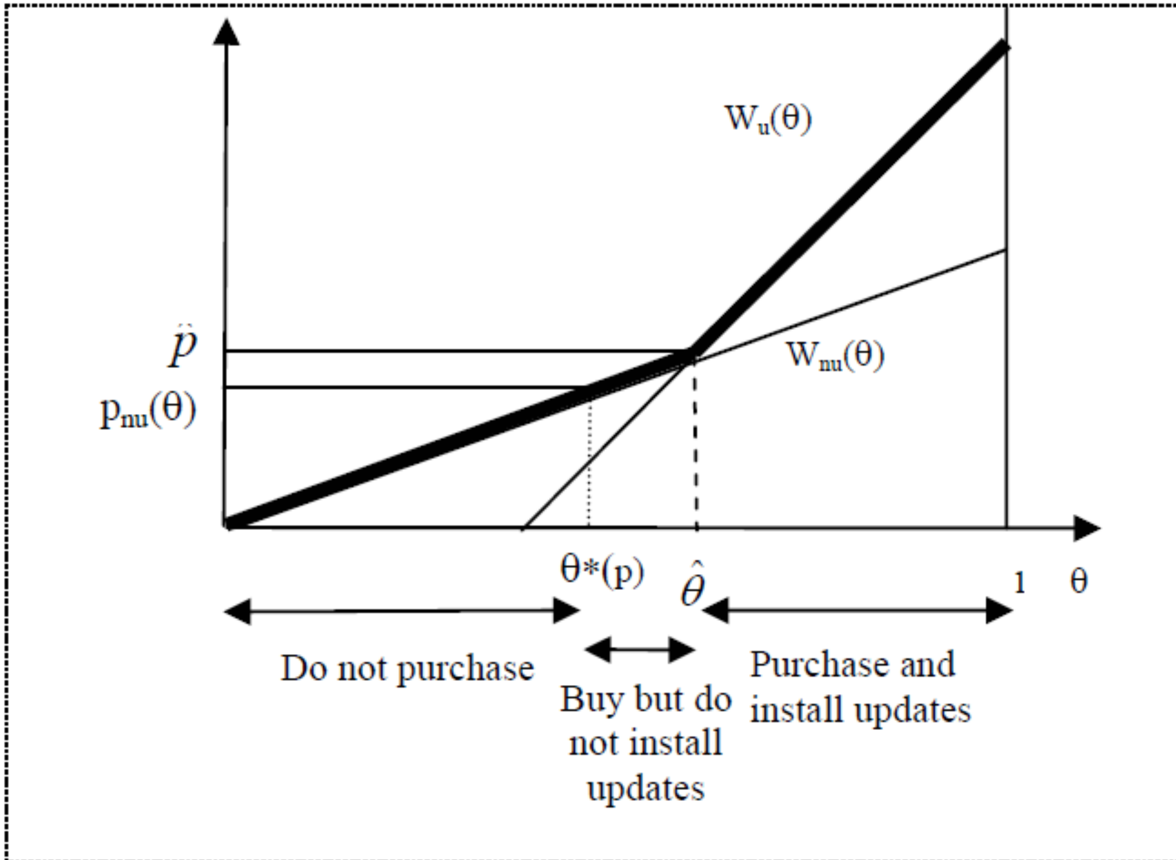
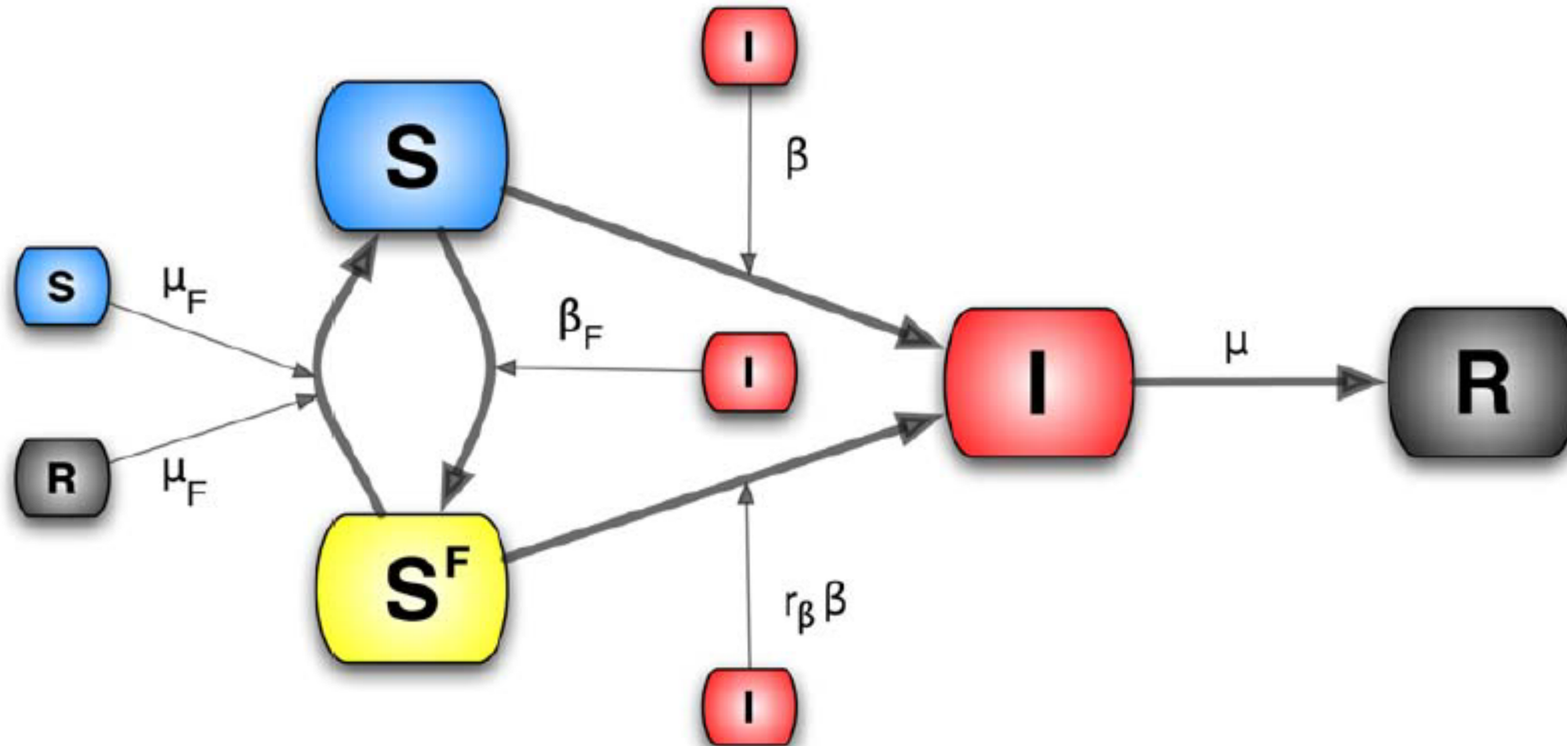
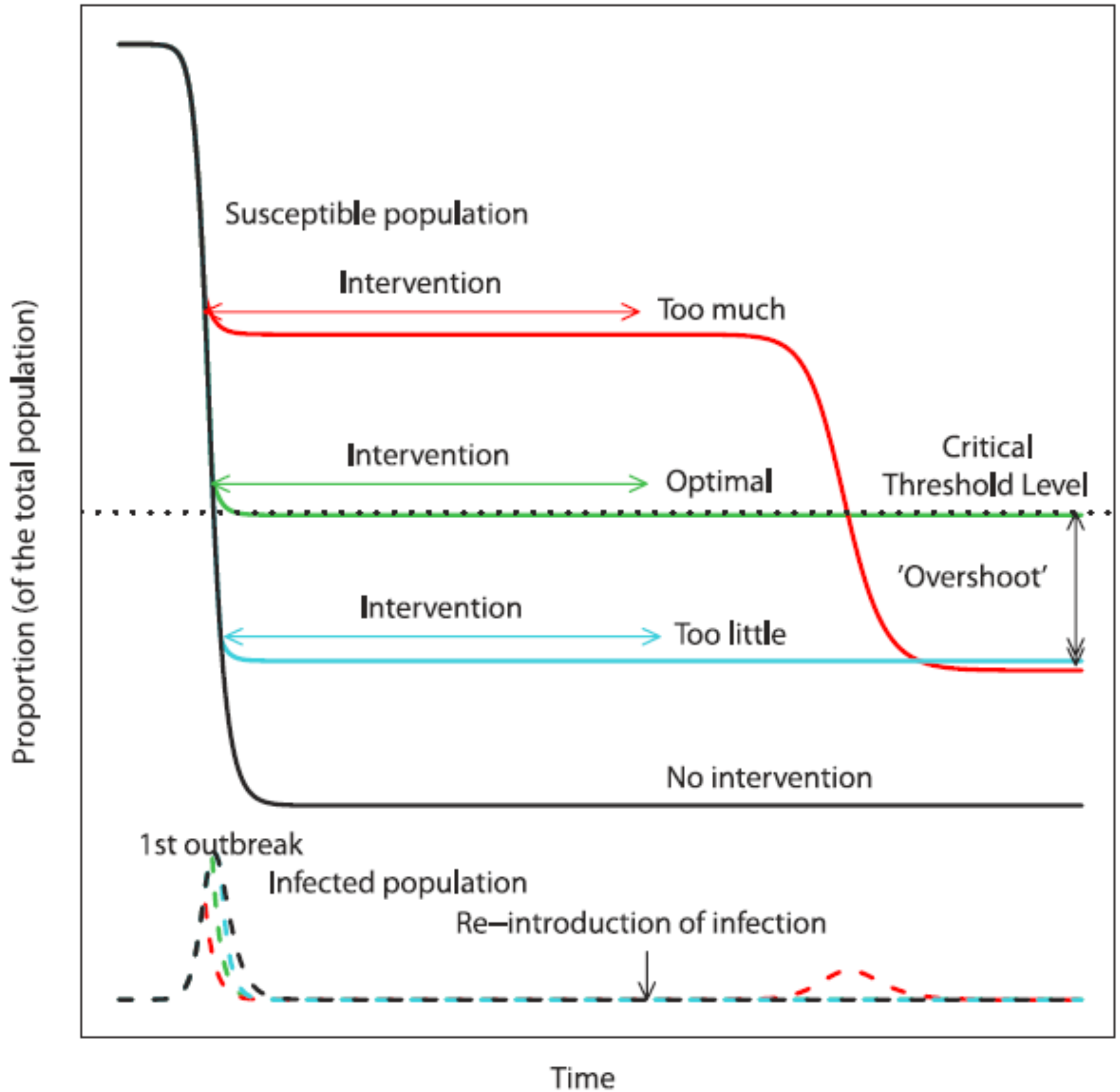


Figure 1: Purchase/Update Decision when Marginal Consumer Type $\theta^*(p) < \hat{\theta}$

Choi, J. P., Fershtman, C., & Gandal, N. (2007). Network Security: Vulnerabilities and Disclosure Policy. *papers.ssrn.com*. Retrieved from http://ssrn.com/abstract=1133779

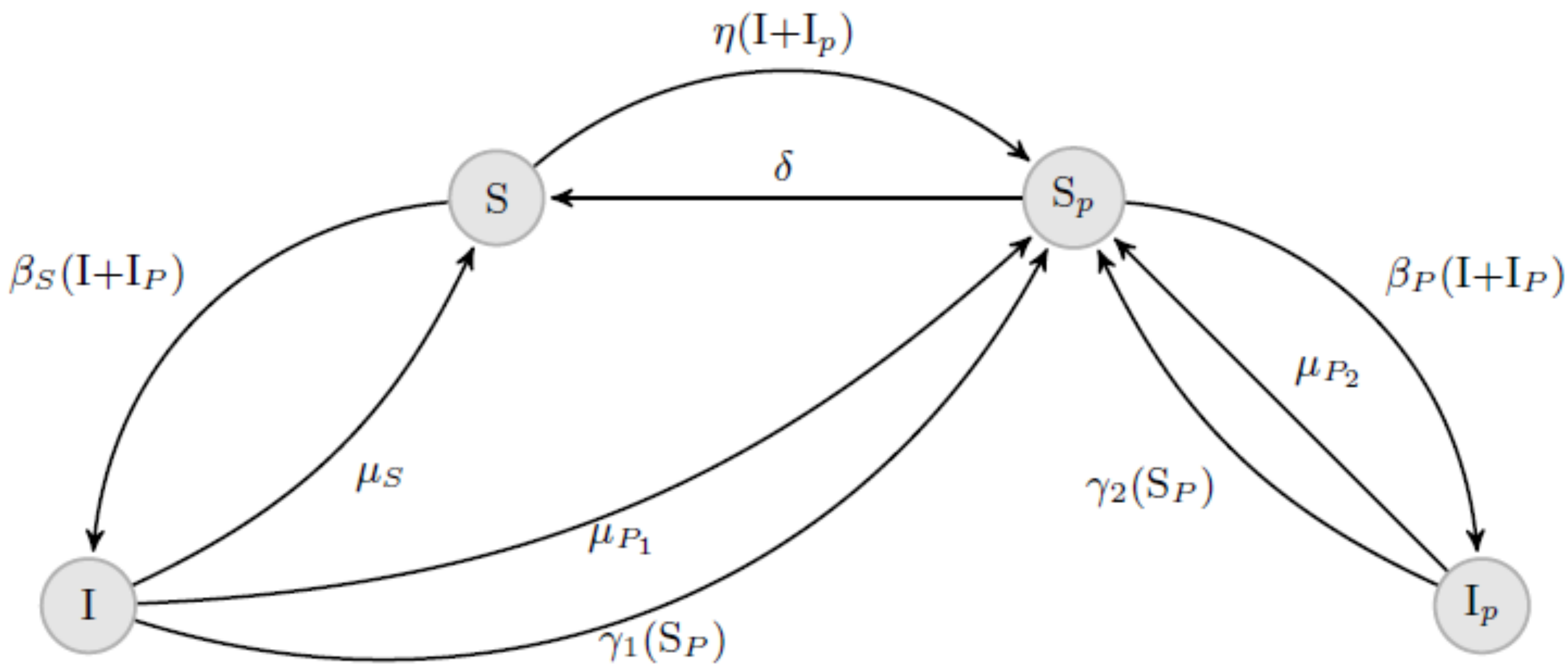


Perra, N., Balcan, D., Gonçalves, B., & Vespignani, A. (2011). Towards a characterization of behavior-disease models. *PloS one*, *6*(8), e23084. doi:10.1371/journal.pone.0023084



Fung, I. C.-H., Antia, R., & Handel, A. (2012). How to Minimize the Attack Rate during Multiple Influenza Outbreaks in a Heterogeneous Population. *PloS one*, *7*(6), e36573. doi:10.1371/journal.pone.0036573

Model Creation and Methodology

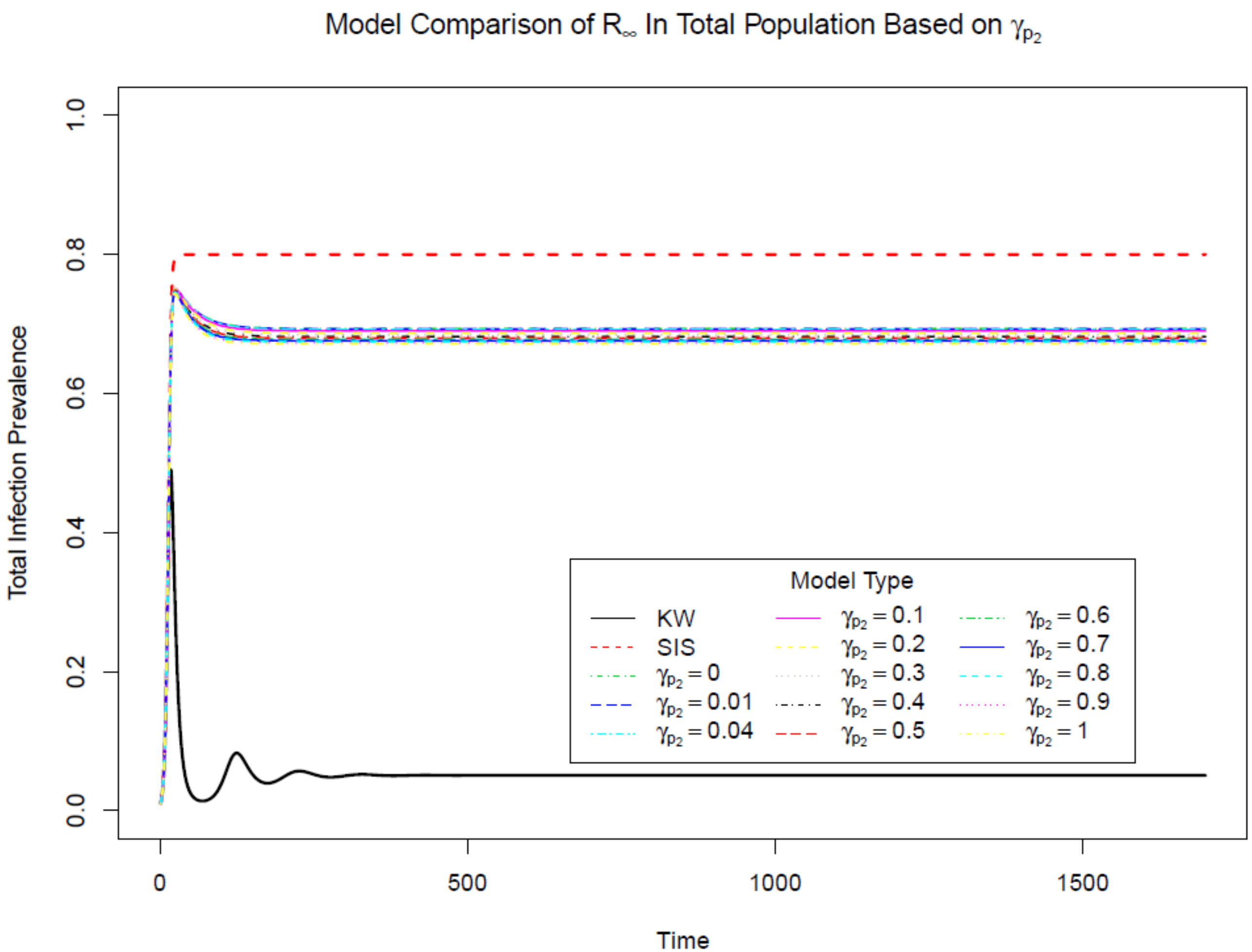


Methodology

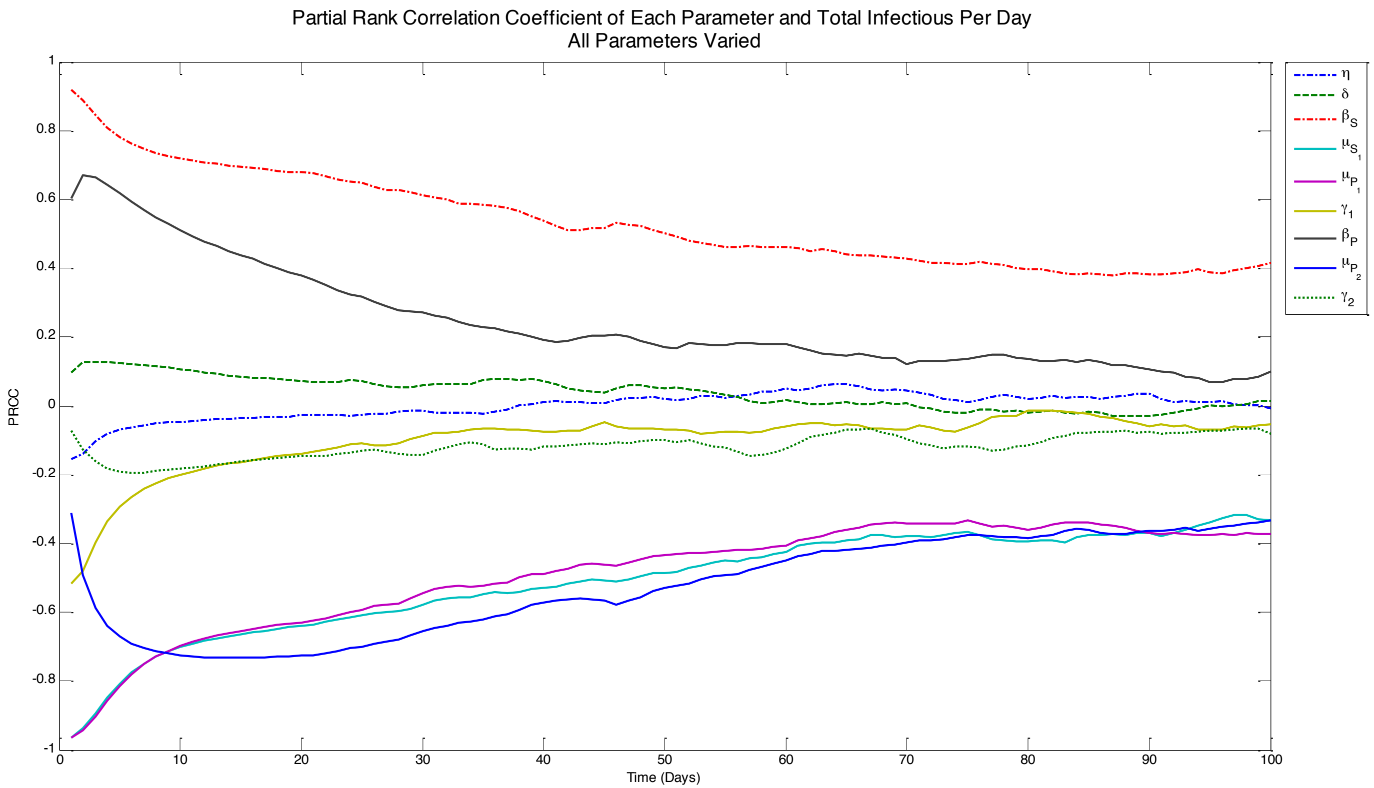
- Variation of single parameter in single population group
- Variation of single parameter in both population groups
- Full Uncertainty and Sensitivity Analysis
- Model Fitting

Results

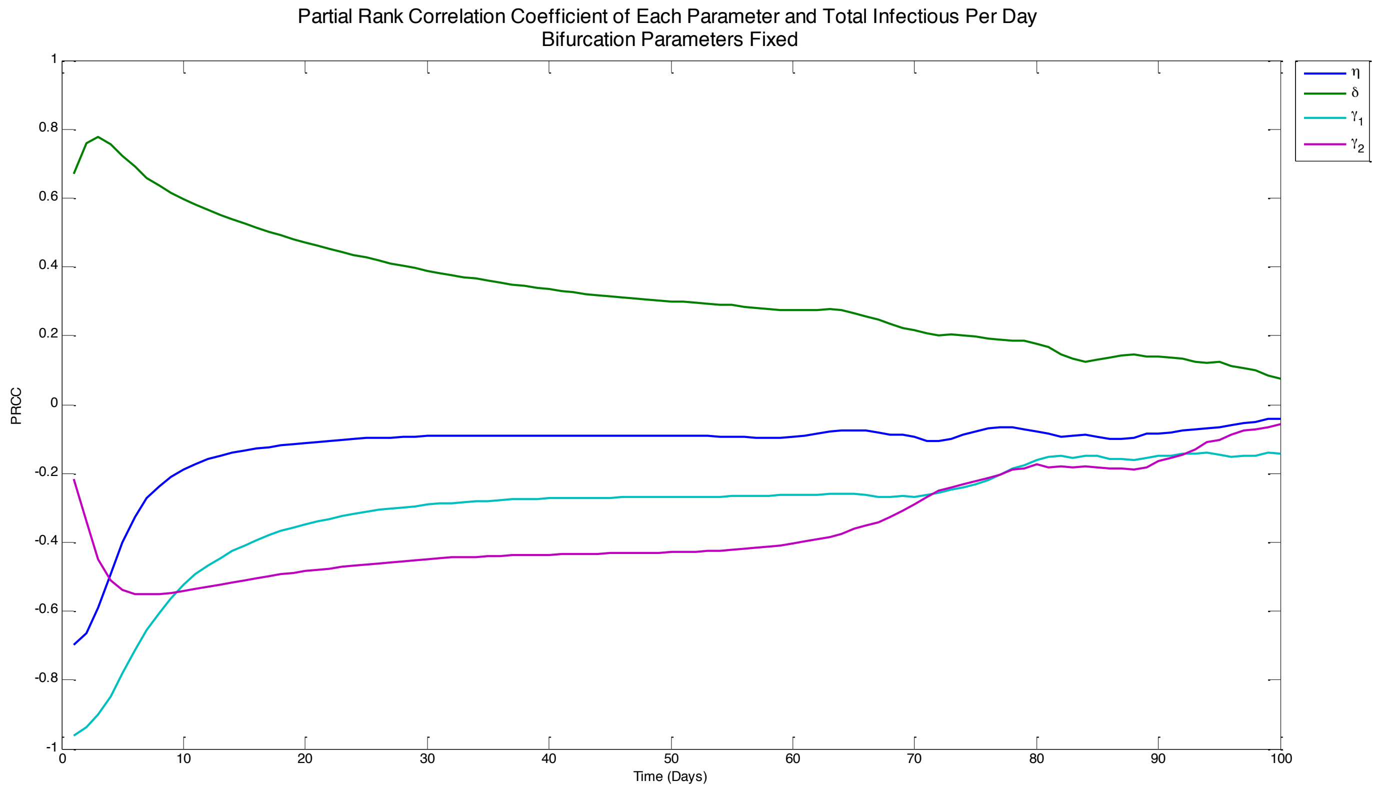
Small groups of risk takers represent a threat to the risk adverse population



Effective contact rates and recovery rates govern whether or not a pandemic occurs



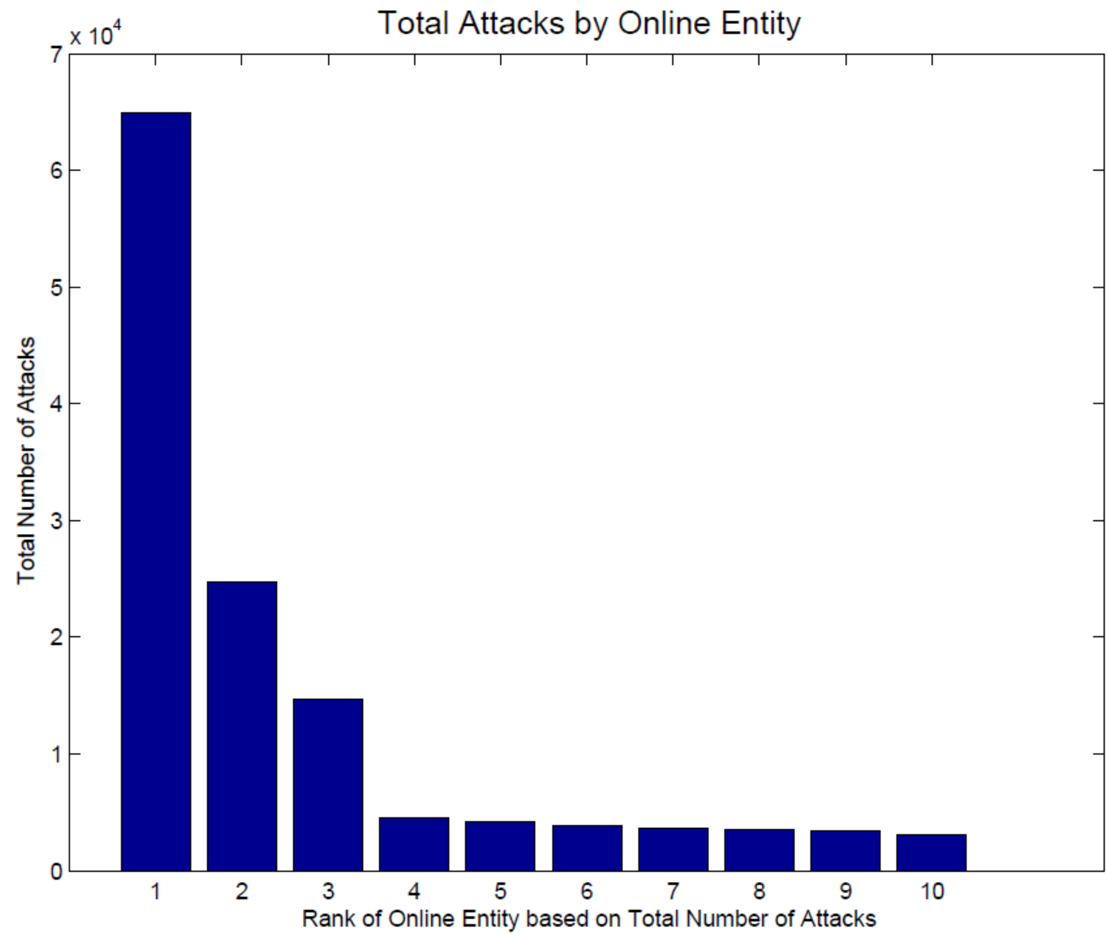
Cost of maintaining risk adverse behavior and recovery due to social response are critical components throughout the lifetime of infection.

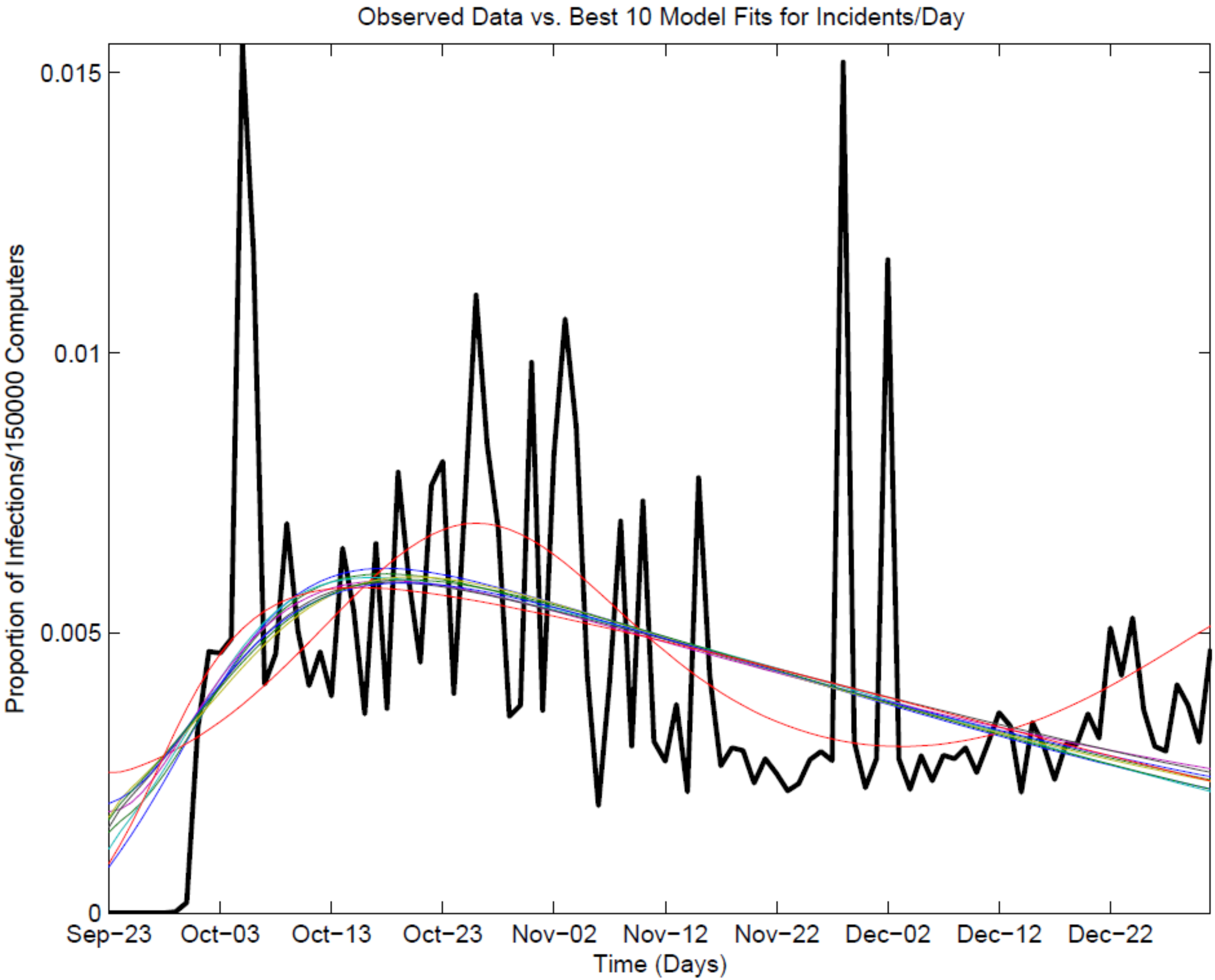


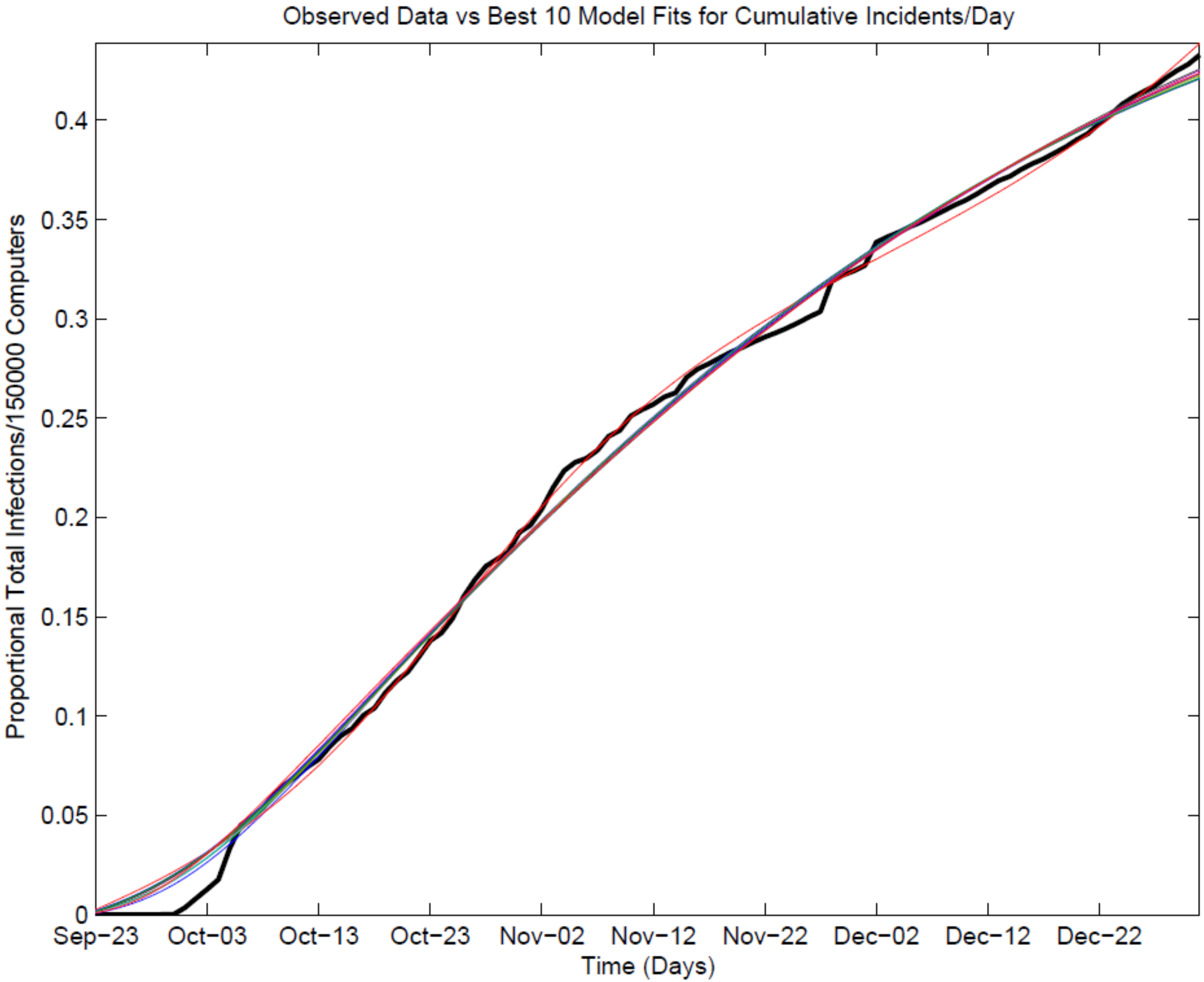
Ability to apply security measures in response to threats is effective in initial stages, but not long term.

Model Fitting

- Top ten spoofed entities account for ~83% of observed attacks.
- Top 20 entities account for ~95% of observed attacks.
- System can be roughly approximated by looking at the top ranked spoofed entity.




Observed Data vs. Best 10 Model Fits for Incidents/Day
Proportion of Infections/150000 Computers
0.015
0.01
0.005
0
Sep−23
Oct−03
Oct−13
Oct−23
Nov−02
Nov−12
Nov−22
Dec−02
Dec−12
Dec−22
Time (Days)



Observed Data vs Best 10 Model Fits for Cumulative Incidents/Day
Proportional Total Infections/150000 Computers
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
Sep−23
Oct−03
Oct−13
Oct−23
Nov−02
Nov−12
Nov−22
Dec−02
Dec−12
Dec−22
Time (Days)

Discussion

- We can look at public health costs due to reduction of coverage

  Franzini, L., Marks, E., Cromwell, P. F., Risser, J., McGill, L., Markham, C., Selwyn, B., et al. (2004). Projected economic costs due to health consequences of teenagers' loss of confidentiality in obtaining reproductive health care services in Texas. *Archives of pediatrics & adolescent medicine*, *158*(12), 1140-6. doi:10.1001/archpedi.158.12.1140

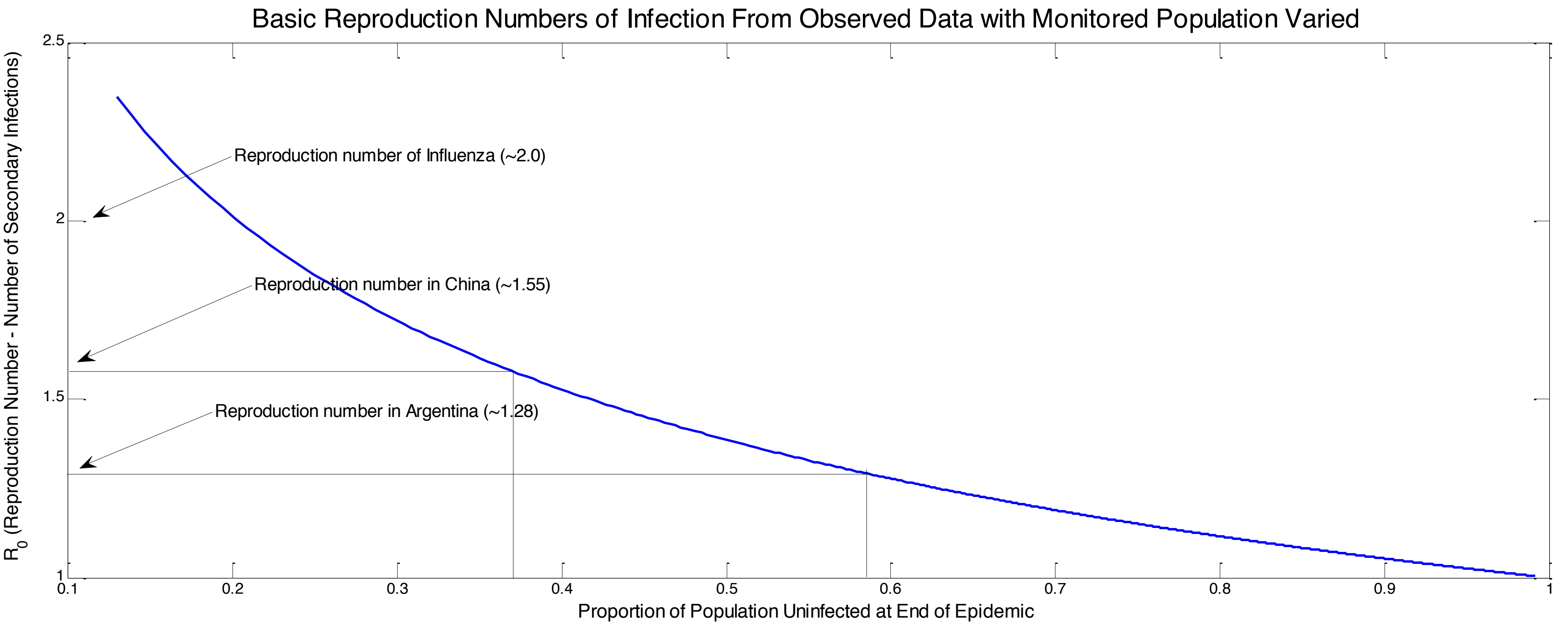
- Effectiveness of Risk Communication

  Spain, J. E., Peipert, J. F., Madden, T., Allsworth, J. E., & Secura, G. M. (2010). The Contraceptive CHOICE Project: recruiting women at highest risk for unintended pregnancy and sexually transmitted infection. *Journal of women's health*, *19*(12), 2233-8. doi: 10.1089/jwh.2010.2146

Conclusions

- A small risk-taking population poses a risk to the risk adverse population
- Ability to recover to a risk adverse population either through social response or individual behavior is effective at reducing global prevalence of malware through the lifetime of infection
- Ability to apply security measures in response to threats is effective in initial stages, but not long term.
- Reducing the effectiveness in users ability to recover to the risk adverse population increases system wide costs.

Real World Results



Questions and Comments

- Thanks to Alessandro Vespignani for advice in model creation
- Thanks to Tyler Moore and Richard Clayton for use of their data set.
- Thanks to the Volkswagen Foundation for travel funding.