

A Framework for Exploring Cybersecurity Policy Options

A proposal for the FTC's PrivacyCon in January 2017

Presenters: **Igor Mikolic-Torreira, PhD**
RAND Corporation

Cortney Weinbaum
RAND Corporation

Headline after headline about cyber breaches tell us that something is not working. Our team at RAND Corporation set out to understand, *With all the cybersecurity tools available, why do failures in the system occur so frequently?* Cybersecurity incentives do not exist and regulation varies from industry to industry, these challenges are apparent. Yet, *Why aren't 'free market solutions'—or non-regulatory solutions—to securing cyberspace flourishing?* RAND Corporation facilitated two cybersecurity 360° Discovery Games, one in the Washington, DC area and another in the Silicon Valley, CA area, to learn why these answers have been so elusive. Our research and results address the following topics within the FTC PrivacyCon areas of interest:

- **Quantifying Consumers' Privacy & Security Interests:** We studied why valuations for privacy and security compete with valuations for speed-to-market and innovation, and why privacy and security lose out in those market dynamics. We will explain why discussions of and mechanisms for privacy have to choose whose privacy to value, and the costs usually entail another actor's privacy or security.
- **Attack Trends and Responses:** Our games included scenarios for ransomware, identity theft, financial breaches, and vulnerabilities to the internet of things, and explored incentives and options for security-by-design and privacy-protecting technologies and behaviors. We explored the inverse relationship between privacy and security—more privacy for some users means less security for the system—and the impacts and market dynamics for these decisions.
- **Transparency and Control:** When decisions to provide privacy or security for one set of actors or users leads to less privacy or less security for another set, our game explored the first- and second-level repercussions and options for mitigations.

We conducted two games with over 100 experts from different branches and levels of government, private-sector IT firms, universities and think tanks, traditional journalism and new media, and civil liberty advocacy groups and foundations, and we discovered that cyber stakeholders compete to achieve different and sometimes opposing goals, acting much like an **ecosystem**. As we analyzed the results from the games and considered cyberspace in this ecosystem context, it became clear that—like species in a habitat—actors in the cyber ecosystem pursue goals that may align, resulting in symbiotic partnerships, or conflict, resulting in competition for resources. This competitive milieu creates a

dynamic environment from which to consider potential frameworks and solutions. We identified four general groups of actors representing the principal players in this ecosystem: *users*, *developers*, *exploiters*, and *securers*.

We analyzed the relationships among these groups and discovered that the ecosystem is out of balance: Some relationships between groups of actors are much stronger than others, leading to incentives that are not balanced by appropriate counter-incentives. We observed an inherent tension between actors as they each act to protect their interests. These interests—which we’ve identified—have something of a zero-sum relationship. For example, the competitiveness that developers seek, including speed to market and innovation, benefits their own interests while also benefiting exploiters because it dissuades investments in security. These dynamics fail to properly incentivize the developer to provide robust security or to adequately compensate the securer.

Our preliminary framework highlights that cybersecurity suffers from a lack of real demand and the consequences this has. Although users want security, they are not yet willing to pay for it, so security is not a priority in the marketplace.

This work was made possible by the Hewlett Foundation and the final report is scheduled to be published by RAND Corporation in 2016.