A FRAMEWORK FOR EXPLORING CYBERSECURITY POLICY OPTIONS

Igor Mikolic-Torreira | Ryan Henry | Don Snyder | Sina Beaghley
Stacie L. Pettyjohn | Sarah Harting | Emma Westerman
David A. Shlapak | Megan Bishop | Jenny Oberholtzer
Lauren Skrabala | Cortney Weinbaum

RAND CORPORATION

For more information on this publication, visit www.rand.org/t/RR1700

Library of Congress Cataloging-in-Publication Data
ISBN: 978-0-8330-9686-9

Published by the RAND Corporation, Santa Monica, Calif.

Cover design by Pete Soriano
Cover images by Fotolia

Preface

Today's cyber environment presents unlimited opportunities for innovation, interaction, commerce, and creativity, but these benefits bring serious security challenges for governments, private organizations, and individual users. The cyber domain has evolved so swiftly that legal, economic, and societal mechanisms for maintaining security have struggled to keep up. Satisfactory solutions that balance the priorities of stakeholders will require building partnerships among public and private organizations, establishing mechanisms and incentives to foster routine information sharing and collective defense, and educating users about their role in thwarting increasingly sophisticated attacks.

The goal of this project was to develop an initial framework for cybersecurity that considers the roles of government, industry, advocacy organizations, and academic institutions and how these stakeholders' concerns relate to each other. In support of this objective, the RAND Corporation developed and conducted a cybersecurity-focused 360° Discovery Game in Washington, D.C., and California's Silicon Valley with participants from government agencies, the technology sector, advocacy organizations, and academic institutions. The games' objective was to foster improved understanding of the positions of the various cybersecurity stakeholders and to illuminate the areas of agreement and disagreement between them. The dynamics of the game play and insights from the participants subsequently informed the framework for the cyber ecosystem. This framework, when fully developed, will support debate and decisionmaking on future cybersecurity policies and practices in an equitable way.

This research was funded by a grant from the William and Flora Hewlett Foundation as part of its Cyber Initiative, which seeks to address a broad range of topics that affect the security, stability, and resilience of a free and open Internet and connected devices. The research was conducted within the Acquisition and Technology Policy Center of the RAND National Security Research Division (NSRD) and the Science, Technology, and Policy program of RAND Justice, Infrastructure, and Environment (JIE). NSRD conducts research and analysis on defense and national security topics for the U.S. and allied defense, foreign policy, homeland security, and intelligence communities and foundations and other nongovernmental organizations that support defense and national security analysis. JIE is dedicated to improving policy- and decisionmaking in a wide range of policy domains, including civil and criminal justice, infrastructure protection and homeland security, transportation and energy policy, and environmental and natural resource policy.

Questions or comments about this report should be sent to the principal investigator, Igor Mikolic-Torreira (Igor_Mikolic-Torreira@rand.org). For more information on the Acquisition and Technology Policy Center, see www.rand.org/nsrd/ndri/centers/atp or contact the director (contact information is provided on the web page). For more information about RAND Science, Technology, and Policy, see www.rand.org/jie/stp or contact the director at stp@rand.org.

Contents

CHAPTER FOUR

CHAPTER FIVE

CHAPTER SIX

CHAPTER SEVEN

APPENDIX

Figures and Tables

Figures

Tables

Summary

The cyber ecosystem—that large body of individuals and organizations connected by the exchange, retention, or shaping of information via digital computing networks—is a system whose impact in the personal and public space continues to grow unabated. Digital capabilities today underpin financial, economic, transportation, energy, and defense infrastructure, but these networks were not built with security in mind. As technology evolves faster than the ability to secure it—with cyber-enabled homes, phones, cars, social circles, work environments, and commerce—the repercussions of compromised networks and exploited data likewise grow more serious and widespread.

How society accommodates and leverages the cyber domain will present strategic choices for the policy community. Policymakers require a framework for designing policies that recognize the priorities of the full range of cybersecurity stakeholders.

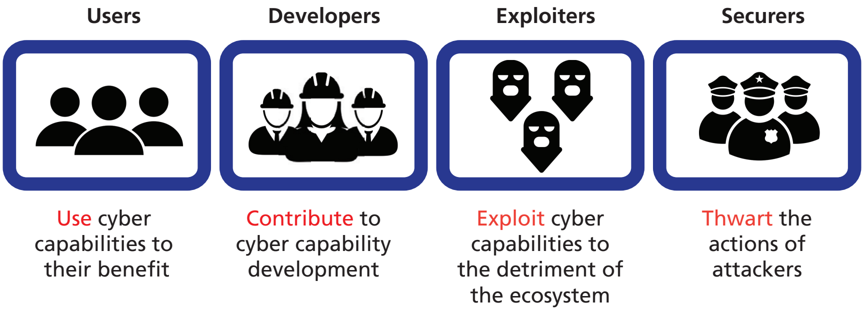
The objective of this project was to develop an initial framework for cybersecurity that considers the roles of government, industry, advocacy organizations, academic institutions, and individuals and how these stakeholders' concerns relate to each other. In support of this objective, the RAND Corporation developed and conducted a cybersecurity-focused 360° Discovery Game in Washington, D.C., and California's Silicon Valley with participants from government agencies, the technology sector, advocacy organizations, and academic institutions. The goals were to explore opportunities for improving cybersecurity, assess the implications of possible solutions, and develop a framework for debating and implementing future cybersecurity policies and practices in an equitable way.

A New Framework for Cybersecurity

Conducting and reviewing the outcomes of the two day-long, scenario-based games revealed that, when it comes to cyber issues, stakeholders contend or compete with each other 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* (see Figure S.1).

We analyzed the relationships between these groups of actors 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 counterincentives. The relationship between securers and both users and developers is imma-

Figure S.1
Four Groups of Cybersecurity Actors


Users
Developers
Exploiters
Securers
Use cyber capabilities to their benefit
Contribute to cyber capability development
Exploit cyber capabilities to the detriment of the ecosystem
Thwart the actions of attackers

RAND *RR1700-S.1*

ture and inadequate. In the game scenarios, there was insufficient demand on the part of users for security. Although users clearly wanted security, they wanted increased capability more. They were unwilling to pay for security in the form of increased costs or forgone capabilities. Likewise, developers failed to see security as a determinative competitive advantage. Security in the capabilities they developed tended to compete unsuccessfully with increased performance or competitive pricing.

We observed an inherent tension between actors and their equities, or priorities and interests. These equities—value for users, competitiveness for developers, and security for securers—have something of a zero-sum relationship. The competitiveness that developers seek benefits their own interests while also benefiting exploiters by dissuading investment in security. As a result, for users and securers, developer competitiveness works against security interests. The security that the securer seeks works to the user's advantage but raises the bar for the exploiter and raises costs for the developer. Similarly, the value that users seek prioritizes performance, capability, and cost over security, which works to the advantage of the exploiter. These dynamics fail to properly incentivize the developer to provide robust security or to adequately reward the securer.

Our framework, preliminary as it is, confirmed the historical observation that cybersecurity suffers from a lack of real demand. Although users want it, they are generally not yet willing to pay for it—so security is not a priority in the marketplace—or to make the additional effort to practice cyber hygiene. While this insight derived from the framework may appear both obvious and elemental, it highlights the framework's capacity to capture the cybersecurity field's "first principles."

Game Design

RAND's 360° Discovery Game methodology immerses a diverse group of participants in an environment in which complex dynamics can be documented, analyzed, and understood. Players engage on a personal, visceral level—similar to real life. Unlike some military wargames, players in a 360° Discovery Game are not competing against each

other; rather, they compete against the scenario in which they have been immersed. As a result, the game incentivizes collaboration, information sharing, and idea generation, because the players' shared goal is to identify solutions that align with each player's equities. By immersing people of disparate backgrounds and responsibilities in a common environment, games can spark or enhance communication and collaboration among those who otherwise would not interact.

We designed the game scenarios with the goal of breaking through perceptual stovepipes that have become embedded in the cybersecurity ecosystem. During each game, we asked participants from a cross-section of disciplines to bring their perspectives to interdisciplinary small-group discussions. Over the course of deliberations, players brainstormed solutions, root causes, key stakeholders, equities, incentives, and impediments to solutions. Players in each game location—Washington, D.C., and Silicon Valley—were presented with the same two scenarios.

Scenario 1: The Dark Side of the Internet of Things

Less than a decade in the future, interconnected devices monitor local environments, automate medication dispensing, improve transportation flow and safety, and perform other valuable functions through what has become a fully developed Internet of Things (IoT). Society has become completely reliant on these devices for efficiency, environmental protection, and maintaining quality of life. But a lack of planning during the IoT's growth has led some manufacturers to stop supporting legacy devices rather than issue security patches and updates. Users who cannot replace these devices—due to the cost or the complexity of integrating updated systems with aging infrastructure—are left vulnerable to security breaches. In this scenario, malicious actors exploit vulnerabilities in the IoT to cause both virtual and *physical* harm. Game participants are challenged to foster a secure environment that delivers the wealth of benefits from the IoT and adequate security to individual users, businesses, and government entities.

Scenario 2: The Erosion of Digital Trust

In this future scenario, trust in the digital operation of financial systems, the marketplace, and commercial transactions has degraded as a result of massive data breaches that hinder most verification and authentication systems. Key data are jeopardized to such an extent that banks and other systems that process transactions are unable to verify the identity of computers and human users, or the validity of the transaction. The scenario places participants in a world in which the compromise of digital credentials has become so widespread that it threatens economic vitality and society's trust in online commerce. Participants are faced with the challenge of rebuilding this trust and increasing the resilience of financial and other essential systems.

Game Results

The games' outcomes and our subsequent analysis led to two primary findings that capture the challenges in aligning the diverse equities of cybersecurity stakeholders.

First, cybersecurity suffers from a lack of real demand in the market. Both producers and users (whether individuals or organizations) generally prioritize performance, capability, and cost over security. Even if security is valued, there is insufficient information for users to make informed security choices. This was consistently noted by the game participants and is reflected in the initial framework we developed based on the games. Second, the cost of breaches falls primarily on the user/consumer rather than on the developer or technology producer, who is largely not held liable. Game participants saw that this fundamental imbalance creates a disincentive for technology developers and producers to prioritize security and that shifting this cost would provide a powerful incentive for the technology producers to prioritize security. However, the games did not provide a clear picture of the nature or mechanisms for such shift, nor did they explore the full implications. These two key game takeaways led us to the missing counterincentives we highlight in our framework.

In both scenarios and in both game locations, participants saw a need for public-private partnerships as part of any framework for addressing core cybersecurity challenges. Silicon Valley game participants saw a greater need for a complete overhaul of how and where business is conducted in the digital age, recognizing that continually patching systems is not a viable approach to long-term security. This group concluded that this lesson applied across all parts of the cyber ecosystem, from individual IoT devices all the way to major systems. In Washington, D.C., participants argued for designating elements of the IoT as critical infrastructure, allowing the government to implement additional protections and security measures to support the health and prosperity of the IoT over the long term. In contrast, Silicon Valley participants had some concerns about government-driven solutions, especially that government solutions would be suboptimal, would be outpaced by a rapidly evolving threat, and might stifle private-sector innovation.

Participants in the Washington, D.C., game questioned the role and authorities of government in protecting the cyber domain, and they debated which agencies have the needed authorities to tackle the challenges raised. Silicon Valley participants talked about "government" as a single entity and focused on the role of consumers in the cyber ecosystem. They saw shifting the cost of breaches from the consumer to the developer or other technology producer as a way to address the device security challenges posed by the first scenario and the identity and trust challenges posed by the second scenario. Participants even suggested a cybersecurity insurance program to cover these costs and create a stakeholder sector in the market that is motivated to improve cybersecurity.

Both games revealed the need to handle high-risk threats differently from low-risk threats. Participants defined high-risk threats as those that could lead to loss of life, such as hacking of medical devices or autonomous automobiles. They defined low-risk threats as those whose only repercussions would be annoyance to users, such as an attack that disables a wirelessly connected kitchen appliance.

Game participants suggested a series of solutions to address a range of threats:

- *Develop cybersecurity standards and certifications*, including standards for cyber positive identification of parties in online transactions as a means of informing users of IoT vulnerabilities and improving the overall cyber security of IoT devices. Cyber identification standards, in particular, would also increase trust in digital transactions.
- *Implement a user's bill of rights*, guaranteeing that users have the information they need to make informed cybersecurity choices when purchasing devices that connect to the Internet. A set of information technolog user rights analogous to the codified patients' rights in the Health Insurance Portability and Accountability Act or the protections provided to air travelers by the U.S. Department of Transportation would serve as a basis for seeking redress when a user's rights are violated. The user's bill of rights was seen as both a mechanism for generating greater market demand for better security and a potential penalty mechanism to encourage compliance among those offering products and services.
- *Encourage information sharing and security benchmarking* between government and industry—and within these sectors—to facilitate action against vulnerabilities and exploits. Information sharing was viewed as critical at all levels (from individual IoT devices to large systems and services). Participants recognized the long history of information-sharing efforts both by the U.S. government and across the private sector, but they emphasized the need to provide information to users about their vulnerabilities and risks, as well as the need to raise awareness among technology producers to enable (and perhaps motivate) remediation.[1]

[1] Note, however, that the U.S. government's historical record in this area is mixed. The current National Institute of Standards and Technology (NIST) framework for the cybersecurity of critical infrastructure (NIST, 2014) has generally been well received. However, the Rainbow Series guides published in the 1980s and early 1990s by the U.S. Department of Defense and, later, the National Computer Security Center were not as well regarded (see, e.g., Schneier, 1994).

- *Provide financial incentives for improved cybersecurity*. These incentives can come in various forms, from "cash for clunkers"–like programs to incentivize end users to replace older, vulnerable, non-updateable devices with newer, more secure devices that will continue to be patched all the way to incentives for device manufacturers to incorporate better security into their devices.
- *Direct research and development funding toward standards development and achieving compliance*. It is not enough to facilitate the development of effective standards. It is also necessary to encourage the development of affordable and effective technology to help consumer devices achieve compliance.
- *Educate consumers*, through either public awareness campaigns or school curricula, on cyber risk and cybersecurity best practices, privacy issues and the implications of sharing personal information, and how to manage privacy and security settings in the cyber ecosystem.
- *Develop a system of security labeling*, similar to food nutrition labels, to allow consumers to compare technology products side by side.[2] Such a move would enable informed consumer choices and potentially create market pressures favoring better security practices, much as crash-test reports help consumers choose safer cars.

Areas for Future Research

The game discussions highlighted a need for policy action in three areas:

- developing a reasonable way to monetize cybersecurity risks
- assigning accountability and liability in the cyber ecosystem
- selecting and empowering jurisdictions to enforce accountability and liability.

[2] This idea potentially goes beyond the work of the CyLab Usable Privacy and Security Laboratory at Carnegie Mellon University (see Kelley et al., 2009) to also "label" security features, capabilities, and the risks of using a device.

These gaps prevent meaningful progress on cybersecurity policy. Game players often assumed—explicitly or implicitly—that these goals could be achieved, yet none proposed viable solutions. All three topics deserve further research and study.

Participants shared many ideas and proposals that raised questions amenable to further analysis. It is worth studying how the following ideas might be implemented, their effectiveness, and their implications:

- the concept of tiered risk—that consequences of cyber attacks on certain elements of the cyber ecosystem are clearly more severe than for other elements
- the role for government in cybersecurity in several areas:
  - government purchasing standards
  - a cyber user's bill of rights
  - cyber education and awareness
  - labeling standards
- designing public-private partnerships, including for security certification and end-user license agreement standards.

Finally, it is possible that American values and preexisting relationships within the U.S. cyber ecosystem influenced participants' discussions. For this reason, future games in different countries or with multinational groups of participants could lead to more varied discussions and results.

The implied zero-sum relationships (zero-sum without infusion of additional resources of the appropriate types) between the equities of users (value), developers (competitiveness), and securers (security) fits within our own research experiences and also parallels similar zero-sum three-way relationships in other fields, such as acquisition (price, performance, schedule). More testing is needed to determine whether this model is both appropriate and useful for considering cybersecurity challenges. For example, it should be tested in a broad set of environments, with a variety of players, and with different scenarios. As we conduct more games, we will explore the implications and inferences outlined in this report, including the nature of the relationships between securers and users and between securers and developers, and whether the value-competitiveness-security dynamic truly represents a zero-sum relationship. If this framework holds up to further development and scrutiny, its broad, high-level nature suggests that it might also provide a way to think about other emerging technologies that are driven by market forces and that could have significant consequences if not developed in a secure manner.

Acknowledgments

Several people and organizations made this project possible. First and foremost, we thank the William and Flora Hewlett Foundation, which provided RAND with the funding to explore cybersecurity frameworks using a gaming methodology. The foundation's goal is to build a field of policy analysis to address problems related to online security, long-term global governance, and technological trustworthiness. In particular, we thank our program officer at the Hewlett Foundation, Eli Sugarman, for his support and encouragement and, especially, for facilitating connections with others across the cyber community.

Richard Danzig and Justice Mariano-Florentino ("Tino") Cuéllar officiated the Washington, D.C., and Silicon Valley games, respectively, calling the games to order and leading the players through each scenario. Their leadership set in motion fruitful discussions and promising connections between participants.

We thank our partners at the Center for Long-Term Cyber Security at the University of California, Berkeley, for hosting our Silicon Valley game and helping to plan and execute that event.

Christina Bartol, Sunny Bhatt, Christina Hansen, Lauren Kendrick, Austin Lewis, Rebeca Orrie, Sarah Soliman, Zach Steinborn, and John Tuten at RAND and Shirish Dhar, Daniel Griffin, Mobin Javed, and Pratik Nadagouda at the University of California, Berkeley, took valuable notes during the games, providing a rich record of the ideas, dialogues, and contrasting opinions that arose when diverse groups of participants collaborated for the first time.

We also appreciate the invaluable contributions of our reviewers: Michael Sulmeyer, director of the Cyber Security Project at the Belfer Center, and our RAND colleague Sasha Romanosky. Their careful reviews and thoughtful feedback significantly improved this report. We also gratefully acknowledge informal comments we received from various colleagues, including Eli Sugarman, Marjory Blumenthal, and Cynthia Cook.

Finally, we thank the players who participated in the two Cybersecurity 360° Discovery Games. We are grateful to them for spending a day of their valuable time with us and for sharing their expertise, experience, and perspectives.

CHAPTER ONE

Introduction

Today's cyber environment presents unlimited opportunities for innovation, interaction, commerce, and creativity, but these benefits bring serious security challenges for governments, private organizations, and individual users. The cyber domain has evolved so swiftly that legal, economic, and societal mechanisms for maintaining security have struggled to keep up. Satisfactory solutions that balance the priorities of stakeholders will require building partnerships among public and private organizations, establishing mechanisms and incentives for fostering routine information sharing and collective defense, and educating users about their role in thwarting increasingly sophisticated attacks.

The goal of this project was to develop a framework for cybersecurity that considers the roles of government, industry, advocacy organizations, and academic institutions and how each group's concerns relate to each other's. The RAND Corporation, in support of this goal, developed and conducted a cybersecurity-focused 360° Discovery Game in Washington, D.C., and California's Silicon Valley with participants from government agencies, the technology sector, advocacy organizations, and academic institutions. The objective of these games was to explore opportunities for improving cybersecurity, assess the implications of possible solutions, in support of developing such a framework for debating and implementing future cybersecurity policies and practices in an equitable way. This report provides an overview of RAND's 360° Discovery Game methodology, why we chose that approach, and how we structured each game. It also presents results and insights from the game participants' small-group discussions, which point to significant opportunities for improving cybersecurity mechanisms and policies and informed a preliminary framework for considering future solutions.

We begin by describing the context of the project's development and the need for a cybersecurity framework. Chapter Two introduces a new framework for cybersecurity that resulted from the outcomes of the games, insights from the players, and the research team's analysis. Against the backdrop of this framework, Chapter Three describes our methodology, how the scenarios and games were designed, how the game players were chosen, and what roles they were assigned. Chapter Four presents outcomes from the first game, which took place in Washington, D.C., and Chapter Five presents outcomes from the second game, in Silicon Valley. Chapter Six highlights similarities and differences across the two games, and Chapter Seven concludes the report with an overview of opportunities for follow-on analysis and research to enable progress in addressing important cybersecurity policy challenges.

The Cybersecurity Landscape

The cyber ecosystem—that large body of individuals and organizations connected by the exchange, retention, or shaping of information via digital computing networks—is an area whose impact in the personal and public space continues to grow unabated. New media and virtual communication are displacing traditional methods for sharing information. Cyber venues (not just Facebook and Instagram, but social sites in the broadest sense of the word) have become a preferred social space for large segments of the population. Wearable technologies monitor human activities and health, and they even observe the local environment. Cyber capabilities underpin financial, economic, transportation, energy, and defense infrastructure. People live in a world of increasingly cyber-enabled homes, phones, cars, social circles, work environments, and commerce. The Internet is ubiquitous as a personal knowledge portal, offering on-demand access to content and an opportunity to interact and create the very content that other users can access on demand. Marketplaces and public services are becoming more accessible and convenient. For all these benefits, there is a tradeoff: With so much valuable data moving through servers and rapidly evolving capabilities to access and exploit them, extremists, criminals, hostile groups, and competing nation-states are finding more opportunities to gain the advantage in cyberspace.

How society accommodates and leverages the cyber domain will present an unavoidable set of strategic choices for the policy community for the foreseeable future. History has shown that policies will likely misconstrue the trajectory of technology-driven change and misread its impact. Policymakers may regret missing opportunities to prevent negative societal consequences. Where they choose to take action, they will be expected to exercise due diligence in plotting an informed and responsive strategy for cybersecurity to maximize the nation's strategic interests. And to do so, they will need a policy formulation framework that captures the equities of the entire cybersecurity ecosystem.

The Need for a Cybersecurity Policy Framework

The William and Flora Hewlett Foundation awarded RAND a grant to develop an expansive and socially relevant framework for cybersecurity policy that accounted for long-term economic impact and societal priorities and facilitated sustainable information technology (IT) development, innovation leadership, national security, and law enforcement.

Starting from this guidance, we developed a cybersecurity-focused 360° Discovery Game, which we conducted in two locations with two sets of stakeholders from across the cybersecurity ecosystem. The game's structure and resulting stakeholder discussions highlighted five overarching policy directions:

1. **Management.** How can governments, businesses, and individuals balance priorities in terms of personal privacy, user convenience, technological innovation, financial incentives for entrepreneurs, and security? Who owns personal data; who decides

how, when, and where they can be used; and who is responsible for protecting them?

2. **Rights.** How can policies best balance access, user privacy, and the good of society? Under what criteria should private data be accessed to investigate security breaches or crimes?
3. **Roles and obligations.** How should the roles and responsibilities of government, industry, and individuals align to optimize benefits and accountability in cyber-related activities? Might different models for accountability and liability encourage better cybersecurity behavior and discourage unsafe behavior?
4. **Governance.** Where do private-sector cybersecurity issues become government issues, and what governance and information-sharing processes are in place for such situations?
5. **Incentive structures.** How does the market reward security and penalize insecurity?

U.S. policy has not been able to resolve these ambiguities and address cybersecurity in a holistic way precisely because perspectives, stakeholders, and equities are stovepiped into competing communities of interest. This lack of integration is a direct result of the absence of an effective framework for understanding disparate priorities, how they interact, and the available tradespace for balancing them.

The best-known contemporary framework for cybersecurity was developed by the National Institute of Standards and Technology (NIST, 2014). Highly regarded, it features industry standards and best practices intended to help organizations manage cybersecurity risks and protect critical infrastructure. But it is different from the type of framework we sought: While it can help private businesses manage cybersecurity risks in a cost-effective way, it would not help answer the questions posed by our study. The NIST framework has a different purpose and could not be adapted as a basis, starting point, or template for our framework.

The policy roadmaps and frameworks from previous technological developments are also insufficient as a template for cybersecurity, because cybersecurity presents several new and unique policy hurdles associated with the uniqueness of the cyber ecosystem. In the online ecosystem, geography, location, and political boundaries are less of a constraint for access but potentially more of a constraint for regulatory efforts. Time is compressed, meaning that actions can occur much faster than humans can respond, so latency is less of a constraint to malicious actors while remaining a fact of policy development. Furthermore, many developments are software-driven, with near-zero replication cost, so cyber capabilities and practices—both beneficial and malicious—often proliferate easily and rapidly. With such scaling, market-driven transactional cost can quickly migrate to near zero, subsequently minimizing the cost of innovation (even if the fixed cost is high, depending on the expertise and toolset that must be developed and maintained). The online environment is also less and less constrained by complexity. The complexity of cyber-enabled actions can exceed human comprehension without appearing to suffer from increased fragility or vulnerability.

CHAPTER TWO

Introducing a Cybersecurity Framework

Cybersecurity ensures the exchange, retention, or shaping of information via digital computing networks in a way that is free of degradation from intended or unintended interference by human or machine. This is the definition that we adopted for this project, and it is the clearest and most widely adopted definition that we could find. We also identified and investigated two primary accelerating factors that have changed the nature of cybersecurity: the explosion in the size and complexity of the Internet and a greater requirement to trust unseen security safeguards to protect private and privileged data.

The goal of this project was to develop a framework for cybersecurity that considers the roles of government, industry, advocacy organizations, academic institutions, and consumers and how these stakeholders' concerns relate to each other. While there is no standardized definition of a *framework* that captures this objective, for our research process, we defined our foundational framework as *the common and inclusive depiction of the field of study (cybersecurity), presented at the highest level of analysis that both delivers meaningful insights and provides a basis for dialogue across the ecosystem of stakeholders.*

Over the course of the games conducted as part of this project, we observed that cyber stakeholders contend with or compete among each other to achieve different and sometimes opposing goals, acting like an *ecosystem*. As we analyzed the results from the games and considered cyberspace in this context, we realized that—like species in a habitat—cyber actors pursue goals that may align with each other, resulting in symbiotic partnerships, or may conflict, resulting in competition for resources. This competitive milieu creates a dynamic environment from which to consider potential frameworks and solutions. Analysis of the cyber infrastructure through which transactions and interactions occur, the bandwidth between nodes, and common communication protocols and programming languages is not enough to understand the broader social implications of cybersecurity policies, which is the ultimate application of a framework that this project sought to develop. Because the 360° cybersecurity games discussed in Chapters Four, Five, and Six focused on understanding the cyber actors and their interactions, creating a venue in which these actors could interact proved very helpful in developing our proposed framework.

By applying the analytical approach employed in the breakout teams to identify top-level stakeholders, their equities, their resulting relationships, and existing structural impediments and available policy incentives, we were able to conceive a preliminary framework from insights gained across the two 360° games. We emphasize that the framework presented here is a work in progress—one that needs to be more fully characterized, better understood, and tested using different groups of players, in different locations, and under different scenarios.

We began developing our framework by collecting noteworthy and universal first-order observations from the game discussions. For example,

- the observation that security will never be guaranteed, leading to a focus on managing risk
- a long-term dominance of market mechanisms over government-imposed regulations resulting from the market's agility in adapting to technology disruptions and generating innovation-friendly incentives
- the weakness (or even outright lack) of a market force favoring security
- the importance of adaptively aligning market forces, based on stakeholders, their equities, and their relationships, so that cybersecurity is appropriately incentivized

- the resulting need for a dynamic balance among stakeholders in the cybersecurity ecosystem.

These observations, in turn, generated second-order reflection on other insights garnered from the two games. An economic ecosystem (and cybersecurity is one such ecosystem) consists of many actors, all of whom act as rational agents, responding to incentives and seeking to maximize their private benefits—exactly what we observed in the games. So, a cybersecurity framework must be represented as a multipolar market (ecosystem), in which interconnected actors interact in observable ways to maximize the benefits available from the environment or other actors. In our framework, key actors trade risks against available incentives. For any actor, the overall benefits available within this market are balanced against other actors' equities and capabilities. For an actor to capture the optimal amount of benefits, it needs to align the ecosystem's market forces to its own equities. Importantly, for the framework to inform policy formulation and analysis, guide government and private-sector action, and remain viable over the long term, potential solutions need to align with market factors.

It should be noted that what we present in this chapter as our foundational framework is intentionally simplistic and fundamental. Starting with our framework definition, presented at the beginning of this chapter, and drawing insights from the two cybersecurity games conducted to date, we sought to maximize three aspects of the framework's application:

- common and inclusive depiction of the field
- highest level of analysis that delivers meaningful insights
- basis for dialogue across the ecosystem of stakeholders.

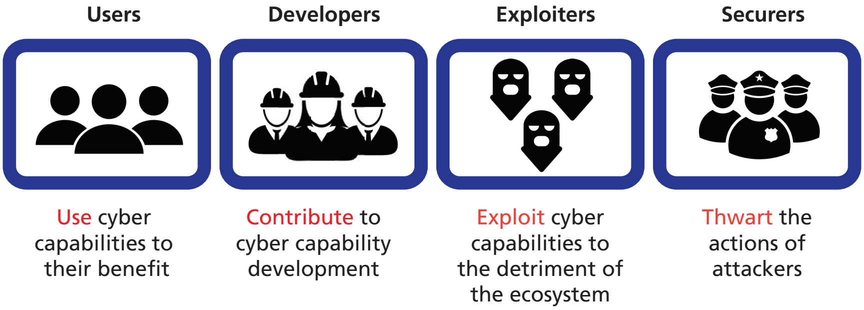
The analysis and supporting background presented in this chapter are informed by these three criteria. All characterizations and properties of the framework are consistent with the participants' collective behaviors and deliberations in the games' breakout and plenary sessions. While the insights derived from the framework might appear both obvious and elemental, we suggest that they are after-the-fact observations, demonstrating the framework's success in capturing the field's "first principles" that it sought to instantiate. Finally, we view this framework as embryonic, one that should mature and develop when subjected to future 360° games and, more importantly, when applied to specific policy formulation activities.

Cybersecurity Actors

We identified four general groups of actors representing key stakeholders in the cybersecurity ecosystem: *users*, *developers*, *exploiters*, and *securers* (see Figure 2.1).

Users are the consumers of cyber capabilities. Their equities include harnessing the benefits of operating in cyberspace (including the ability to transact commerce reliably) for purposes of productivity, empowerment, and overall utility. The speed of action, lower transactional costs, ability to connect with others independent of physical distance, and scalable access, movement, and storage of information are all benefits that users value. *Developers* are those who meaningfully contribute to the generation of cyber capabilities, enabling users to leverage existing or new cyber capabilities for their own benefit. These capabilities can take the form of software, hardware, online services, intellectual property, system support to specific operations, or improvements in the efficiency

Figure 2.1
Four Groups of Generic Cybersecurity Actors


Users
Developers
Exploiters
Securers
Use cyber capabilities to their benefit
Contribute to cyber capability development
Exploit cyber capabilities to the detriment of the ecosystem
Thwart the actions of attackers

RAND *RR1700-2.1*

or effectiveness of the larger cyber ecosystem. *Exploiters* are those who use cyberspace to extract value from the ecosystem, many times from users, and do so in such a way that they work against the best interest and health of the larger ecosystem. This category includes those who act with negative intentions or operate outside the law or the accepted norms of behavior. Some cyber actors may have good intentions, but they fail to recognize the negative impact of their actions beyond their own self-interest. Those actors who rationalize their behaviors as either within their own subgroup's norms of behavior or serving a mistakenly greater good can also fall into this category. Finally, *securers* are actors whose actions and interests revolve around making the ecosystem more defendable and resilient. They may serve large groups or single users by making their cyber activities more secure. They provide these users with the confidence to conduct transactions in cyberspace that may otherwise expose them to risks. Securers may do this by providing systems or techniques to lower exposure, increase situational awareness, or, on rare occasions, impose costs on exploiters. They may also provide intangible security by effectively advocating for users' rights, the long-term benefits of privacy, or the value of multi-stakeholder governance within the ecosystem.

These four categories of actors are painted with a broad brush, and precise boundaries have not yet been defined. A specific person or entity might be classified in one group in a given situation but another group in a different situation. For example, a search engine company may collect and store massive amounts of user information in a secure manner (such as by using end-to-end encryption, isolated key codes, certificates, or passwords) to enhance end users' search results or shopping experiences. Meanwhile, that same search engine company might sell the accumulated personal identifying information and user-preference data to a third party.[1] The user may not be able to decipher an end-user license agreement (EULA) specifying these terms.[2] If the

[1] This "trail of crumbs" and other sources of open intelligence make it easier to exploit a user's accounts (Bazzell, 2014).

[2] A EULA is a legal contract between a software application author or publisher and the user of the application. In most cases, the software provider sets the EULA's terms, and

third party were to use these data against the best interests of users, it would be an exploiter, while the search engine company would simultaneously be a developer and an exploiter, due to its failure to protect valuable data.

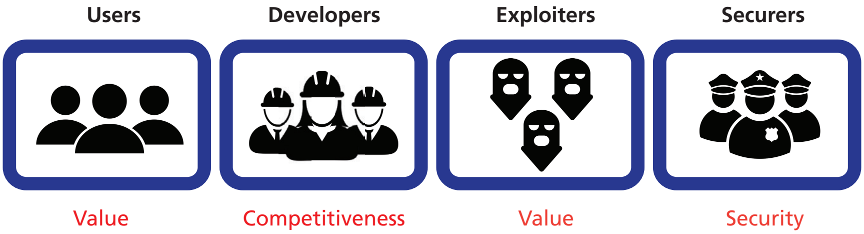
Additionally, in a given scenario, analytical task, or policy assessment, each class of actor could represent individuals, groups, or organizations. Likewise, actors are parsed into one of these four types relative to their equities and relationships with respect to the issue being examined. While they may perceive or rationalize their intent as benign, what matters for the purpose of binning actors into these four groups is the cumulative effect of their actions in the context being examined.

Equities and Relationships

As in all ecosystems, actors in the cyber ecosystem seek to maximize their own interests. In our preliminary cybersecurity framework, we define *equity* as actors' interests based on their desire to maximize the benefit they derive from the ecosystem. For users, their equity involves maximizing the value they get from the cyber ecosystem—whether it allows them to engage in activities they could not do before or to operate better, cheaper, easier, or faster. Developers seek to maximize their competitiveness within the cyber market, such as by providing better capabilities, increasing profits, gaining wide user acceptance, or being acknowledged for uniqueness or quality. Exploiters seek to extract value from the ecosystem, principally at the expense of users. The value they seek can be economic, or it can be to manipulate and gain influence over users. State-based exploiters might have political or military motivations. Securers' equity derives from thwarting the actions of exploiters. Securers find value in making some aspect of the cyber ecosystem more secure from exploiters than it would be otherwise. These equities are illustrated in Figure 2.2.

the user can either accept and use the software or reject the terms and be denied access. The user very rarely has any flexibility to choose terms or conditions. For further examination of problems common to privacy policies and EULAs, see Luger and Rodden (2013) and Hartzog (2013).

Figure 2.2
Cybersecurity Framework Equities



RAND *RR1700-2.2*

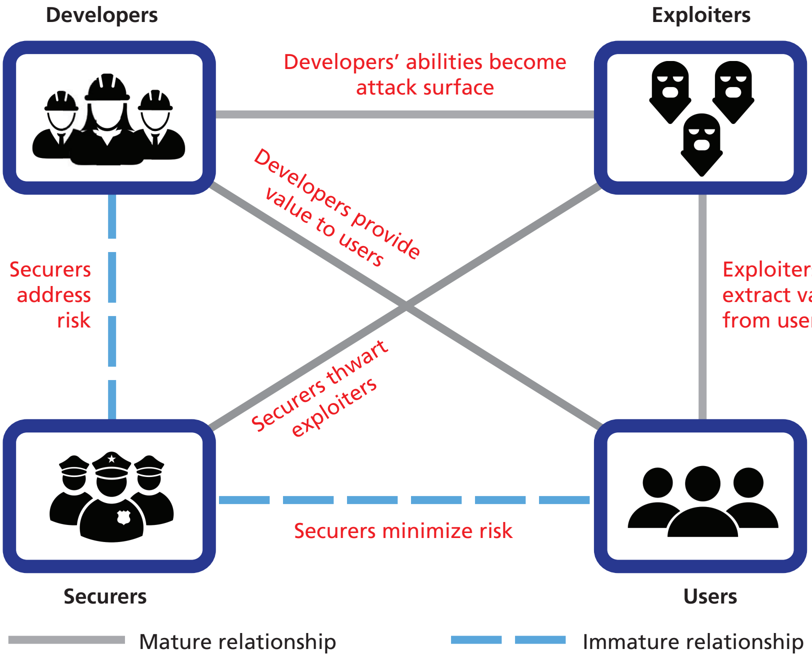
Based on their equities, each of the actors has a relationship with other actors. Users employ the capabilities developed by developers, they are targets for exploiters, and they rely on securers to help them thwart exploiters. Developers provide value to users, the capabilities they develop provide a target for exploiters, and they rely on securers to reduce risk within the ecosystem. Exploiters extract value from users, leverage capabilities generated by developers, and attempt to elude the efforts of securers.[3] Securers increase security for users, lower risk for developers, and thwart the actions of exploiters. These relationships between actors are shown in Figure 2.3.

The developer-user relationship is actively exercised and is a driving force in the market today. Likewise, the exploiter-user relationship results in a cybersecurity challenge, and the securer-exploiter dynamic has the attributes of a cat-and-mouse game. While some of these relationships have negative manifestations, each shows some of the characteristics of maturity and bilateral balance.

Yet, during the games, we discovered that the ecosystem is out of balance in various ways. This notion came through in various contexts during the game play. For example, there is an imbalance between producers and users in covering the costs of data breaches, an imbal-

[3] Readers who are interested in technical analyses of exploitation are encouraged to explore the many books, papers, and lectures on the topic, including Kim's *The Hacker Playbook 2: Practical Guide to Penetration Testing* (2015), Zalewski's *Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks* (2005), and Bazzell's *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information* (2014).

Figure 2.3
Today's Cybersecurity Framework Relationships


Developers
Exploiters
Developers' abilities become attack surface
Developers provide value to users
Securers address risk
Exploiters extract value from users
Securers thwart exploiters
Securers minimize risk
Securers
Users
Mature relationship
Immature relationship

RAND *RR1700-2.3*

ance that arises when responsibility for cybersecurity lies with a party other than the one that incurs risk, and an imbalance between market demand for new capabilities versus better security. The relationship of the securers to both users and developers is both immature and insufficient. In the scenarios presented in the games, there was insufficient demand on the part of users for security. Although users clearly wanted security, they wanted increased capability more. They were unwilling to pay for security in the form of increased costs or forgone capabilities. Likewise, developers failed to see security as a determinative competitive advantage. Security in the capabilities they developed tended to compete unsuccessfully with increased performance or competitive pricing.

We observed an inherent tension between actors and their equities. These equities—value, competitiveness, and security—have something of a zero-sum relationship (without the infusion of additional resources).[4] The competitiveness that developers seek benefits their own interests, but it also benefits exploiters by dissuading investment in security. As a result, for users and securers, developer competitiveness generally works against security interests. The security that the securer seeks works to the user's advantage but raises the bar for the exploiter and raises costs for the developer. Similarly, the value that users seek prioritizes performance, capability, and cost over security, which works to the advantage of the exploiter. These dynamics fail to properly incentivize the developer to provide robust security or to adequately invest in what the securer produces. In fact, there is little natural demand today from the other actors for what the securer produces, and this causes an imbalance to the overall ecosystem.

As has been observed repeatedly in the literature and highlighted during the games we conducted, it is clear that cybersecurity suffers from a lack of real demand.[5] Although users want it, they are not yet willing to pay for it by prioritizing security in the marketplace or to make the additional effort to practice cyber hygiene. So, the question is how to encourage these relationships to evolve in a way that generates greater demand from developers and users for what the securers produce.

Incentives and Impediments to Informed Policy

One objective of the framework is to lay a foundation for informed policy. Central to formulating this foundation is discerning existing

[4] It is worth noting that, while additional resources are a necessary condition, they alone would not be sufficient. A number of states and multinational organizations have attempted to recreate the types of "innovation miracles" for which Silicon Valley has become known by applying resources in the form of funding and guidance—but without success. For this reason, one of the six breakout groups in each game focused on the challenge of sustaining a climate of technological innovation while addressing the cybersecurity challenges presented in the scenarios. See Chapter Three for a complete description of the game structure and breakout session tasks.

[5] See Chapter 6 of the National Research Council's *Computers at Risk: Safe Computing in the Information Age* (1991) for an early discussion of how market forces fail to reward security.

incentives for appropriate policy and impediments to the formulation of such policy. With only two cybersecurity-themed 360° Discovery Games to draw from, any identification or characterization of these incentives and impediments is both rudimentary and tentative. That said, we were able to make a number of observations. Regarding incentives for the three actors of interest (users, developers, and securers), all have a common stake in the continued development, capability, and maturation of the ecosystem and in ensuring that it is not stunted by the actions of exploiters. Their common longer-term interests lie in solutions that do not violate societal values. They prefer market-based rather than authoritarian solutions.

Authoritarian, or government-imposed, solutions that are contrary to market forces appear doomed to ineffectiveness in the long term. Since all such government-imposed solutions would, by definition, be state-based, they would also be localized geopolitically. But the cyber ecosystem is stateless. Therefore, state-based solutions that attempt to control, or even influence, the behavior of actors will compete against alternative, stateless solutions. For example, a government could mandate that developers under its jurisdiction take certain actions, but in the global marketplace, those developers are subject to other countries' laws and may be competitively penalized by implementing their own state's suboptimal solution. Therefore, that government would effectively drive users away from developers in their own country. This is a particular concern because it is so easy to cross national and political boundaries in the cyber ecosystem. Such a policy action is unlikely to be effective and would probably be costly; it could also lead to a loss of national cyber capabilities and a greater reliance on external developers, generating uncomfortable national security trade-offs. Likewise, a government can be perceived as an exploiter when it prioritizes national security interests over user privacy and developer autonomy. In this case, the government's influence in the ecosystem is diminished.

Even the concept of *jurisdiction* is ambiguous in the cyber ecosystem: Government efforts that force companies to store personal data on local servers or that require source code and related intellectual property to be disclosed for review illustrate how laws and regulations in one nation may affect the conduct of vendors headquartered in another. Such mandates also lead global businesses to behave differently in different countries.

Rather than offering top-down solutions, it appears that governments are best suited to provide or align incentives for improved cybersecurity. A potent incentive available to governments is facilitating multistakeholder processes to address and characterize problems and recommend solutions that account for a broad range of equities. However, incentives are not automatically *good*, and the line between mandates and incentives can blur in practice when incentives are heavy-handed and not carefully thought through.

Based on observations from the two games conducted to date, it appears that *credible information* regarding cyber risk and organizational performance could transform the two biggest impediments to a more secure ecosystem into incentives. Currently, users are unwilling to prioritize greater security, but that may be because they lack easily digestible information about how to protect their cyber activities and interests by practicing good cyber hygiene and how to discern which developer's systems are most secure. Developers are unwilling to prioritize security because they lack viable risk information and consequences when breaches occur. These impediments could become incentives if the challenges highlighted in the following chapters are meaningfully addressed.

CHAPTER THREE

360° Discovery Game Methodology

To develop the foundational framework for the development of viable cybersecurity policies, we created two scenarios based on the cybersecurity concerns discussed in the previous chapter and incorporated them into a serious discovery game. Analytical games conducted in a professional environment are generally designed to identify the "how" and "why" of a complex situation or condition, particularly one in which human engagement plays an important role. Much of what we sought to analyze and explain in this project was emergent behavior when groups interact in a policy formulation context. We were interested in examining not just consensus outcomes or points of disagreement but also the interactions of many choices by many participants in the shadow of uncertainty.

We chose to use RAND's 360° Discovery Game methodology because it allowed us to generate an immersive environment in which these dynamics can be documented, analyzed, and understood and in which players engage on a personal, visceral level—similar to real life. Unlike some military wargames, the players in a 360° Discovery Game do not compete against each other; instead, they compete against a scenario in which they have been immersed. As a result, collaboration, information sharing, and idea generation are all incentivized, since the players' shared goal is to create solutions that align with each player's equities. By immersing people of disparate backgrounds and responsibilities in a common environment, games can spark or enhance communication and collaboration among those who otherwise would not interact. A 360° Discovery Game can also explore a specific problem that may be too poorly defined or understood to be probed in other ways.

We designed the following scenarios with the goal of breaking through the perceptual stovepipes that have become embedded in the cybersecurity ecosystem. In this type of game, the scenario itself is the opponent, and players are challenged to solve the problems that the scenario presents.

Scenarios

The games introduced the players to two scenarios set in the year 2021, with each scenario postulating a different series of potential cybersecurity crises.[1] After providing an overview of cybersecurity's future "history" through 2021, we presented participants with a series of scenario-associated challenges replicating the conditions of a real-world crisis.

Scenario 1: The Dark Side of the Internet of Things

The first scenario in the cybersecurity exercise postulated a world in 2021 in which the Internet of Things (IoT) has become essential to business and day-to-day living but overrun by malicious actors. Hackers have created new means of spying and extortion through any device connected to the IoT, while hostile governments have a greater ability to threaten individual Americans and the U.S. government.

Connected devices have become ubiquitous—in homes, offices, factories, and vehicles and even on our persons—yet they lack sufficient security and privacy controls to protect their users. In the 2021 scenario, IoT devices monitor local environments, automate medication dispensing, and track and improve transportation safety. At the same time, society has become completely reliant on these devices for efficiency, protecting the environment, and maintaining quality of life.

[1] While these scenarios were generated by RAND staff, interested readers can find additional valuable material in such sources as Goodman's *Future Crimes* (2015) or Schneier's *Data and Goliath* (2015).

Most IoT devices were not designed with security in mind. Making matters worse, a lack of planning when the IoT began growing in the 2010s means that some manufacturers have chosen to stop supporting devices rather than issuing necessary security patches and updates. In the intervening years, when manufacturers went bankrupt or abandoned a product line, their products effectively became orphaned, lacking support and updates. Users who cannot afford to replace obsolete devices and commercial or government users whose devices are embedded in complex and aging infrastructure are left vulnerable to security breaches. As a result, users are subject to abuse and exploitation by malicious actors in the form of extortion, blackmail, or physical harm via IoT devices. Even individuals fleeing abusive relationships or totalitarian regimes can be traced, harassed, and threatened.

A key element of this scenario is how malicious actors could use the IoT to cause both virtual and *physical* harm. This scenario places players in a world in which malicious exploitation of the IoT has become common and socially and economically disruptive. The public outcry over these malicious activities—as well as government officials' concern about malicious activities not known to the public—has led to an impending crisis requiring action at the national level.

In this scenario, neither abandoning the IoT nor accepting the status quo is an acceptable outcome. These technologies are too important to the day-to-day functioning of society, and the negative impacts of hackers must be addressed.

Scenario 2: The Erosion of Digital Trust

The second scenario envisioned a world in 2021 in which systems designed to authorize or deny access to computer systems and the systems used to conduct daily transactions have broken down. Trust in the financial system and security marketplace has been lost. That loss of trust was due to the speed of transactions in the digital world; systems that were built to hold, process, and collect individual information; and the fact that systems used to carry out transactions were no longer able to maintain trust. Players were faced with the challenge of rebuilding that trust and increasing the resilience of financial systems.

Successful transactions depend on trust in third-party credentials. In the physical world, in Western countries, this trust is established with drivers' licenses, birth certificates, and credit cards. In the digital world, credentials include usernames and passwords, personal identification numbers (PINs), unique code-based keys, answers to "private" questions, and biometrics. Similarly, consumers trust ATMs, financial networks, and payment processors to accurately and faithfully execute transactions.

As malicious actors acquire increasingly large and expansive sets of personal information and are able to aggregate and correlate them, they are increasingly able to compromise digital credentials. For example, they could know an individual well enough to answer private questions, determine passwords, and even acquire digital biometric information. Previously compromised data sets continue to provide information, and businesses and financial institutions must engage in even more intense questioning to confirm a user's identity.

A combination of social engineering and information culled from massive data breaches allows malicious actors to target specific individuals or to compromise mass numbers of identities, as seen in previous hacks against the U.S. Internal Revenue Service and Office of Personnel Management, and, in the scenario, in entire state systems for drivers' licenses and birth records. In the scenario, this has resulted in a kind of authentication spiral. When companies cannot trust that purchasers are who they claim to be, the company will require more information. By 2021, so much personal information has been compromised that traditional authentication systems become meaningless, opening the door to more breaches. Data analytics make it easy to crack security questions for an individual account, while vast databases of hacked information make it easy to take advantage of millions of accounts simultaneously. Furthermore, rapid advances in 3D printing technology and the sophisticated technical capabilities of criminal networks facilitate the forgery of physical identity documents, such as drivers' licenses. Criminals—or nation-states—can easily generate drivers' license that can pass most, if not all, tests used by security services. These documents are "real," containing real data from a real government database.

The problem is exacerbated in the scenario when malicious actors also compromise key networks that underlie the financial system, including major payment processors. By compromising the financial infrastructure itself, criminals can siphon off small "fees" on every transaction, divert transfers to illegitimate third parties, or even initiate phony transactions. As a result, even simple transactions, such as ATM withdrawals, direct deposits, and electronic bill payments, become untrustworthy. Individuals can no longer trust that their paychecks will be deposited reliably or that their automated mortgage payments will be made as scheduled. The ensuing loss of confidence in financial systems has a significant economic impact on individuals and businesses.

This scenario places players in a world in which the compromise of credentials and underlying transaction systems has become sufficiently widespread that it threatens the trusted transactions on which commerce and society depend.

Players

When designing the games, we considered the equities and biases of players, with the goal of recruiting a cross-section of players representing competing and conflicting goals and interests. To ensure that we captured a representative sample of players, we designed and developed a taxonomy of cyber stakeholders with a view across the spectrum of nonmalicious actors. Malicious actors were intentionally omitted for three reasons. First, their goals and motivations are already the subject of other research efforts.[2] Second, in these games, the *actions* of malicious actors (e.g., stealing credentials) were more important than their *goals* (e.g., to sell those credentials or use them for other malicious acts), and these actions were pre-scripted in creating the scenarios. And third, including malicious actors as participants in the 360° games

[2] RAND has conducted extensive research on the tactics, motivations, and goals of hackers and other malicious actors, as well as the effects and potential evolution of attacks. For more on the former, see Ablon, Libicki, and Golay (2014); Ablon (2015); Libicki, Ablon, and Webb (2015); and Libicki, Senty, and Pollack (2014).

posed serious problems in providing a focused environment to reveal and explore the equities of cybersecurity stakeholders—the focus of our games. Table 3.1 shows the categories and roles of the stakeholders.

We used this taxonomy to develop invitation lists for each game, ensuring that all groups were represented. Our goal was for each stakeholder group to be represented, rather than to have equal numbers of players from each group. In the real world, these groups are not equal in size. For example, there are always fewer orthogonal thinkers, academics, and advocates than IT producers and users, as the former groups are conducting analysis on and creating policy for the latter. Instead of equal representation, we strove to include each group while creating an environment where they could share their perceptions, equities, biases, and goals.

Each game brought together 50–60 experts from top-tier organizations across each of the stakeholder groups listed in Table 3.1, including officials from different branches and levels of government, private-

Table 3.1
Stakeholder Roles in the Cyber Ecosystem

Stakeholder	Role
IT producer	Develop new IT capabilities
IT security	Secure IT capabilities
Economic	Economists and financiers
Government	Regulators, national security experts, law enforcement, and other government functions
Orthogonal thinkers	Strategic thinkers who consider the unobvious or unintuitive repercussions of changes to the ecosystem
IT users	Use or benefit from new capabilities
Academic and think tank	Conduct research on and in the ecosystem
Advocates	Promote a specific position, such as protection of civil liberties or privacy
Public face	Shares knowledge through the media, writing articles, or maintaining blogs
Legislative and judicial	Creates, upholds, and interprets laws

sector IT producers and users, technology and policy experts from universities and think tanks, journalists from both traditional and new media, and leaders from civil liberty advocacy groups and foundations. Each game adopted the Chatham House Rule, in which any attribution to individual players and organizations is withheld from proceedings and other records to promote uninhibited dialogue.

After each scenario was presented, players were split into six teams of approximately ten players each. Each team was assigned a specific perspective from which to address the scenario challenges. The six perspectives were organized according to three overarching goals, each corresponding to two of the perspectives. The three themes reflect three macro-level approaches that can be used to deal with cybersecurity challenges:

- **Deter and defend against malicious activities.** For our purposes, we separated *deter and defend* into two subgroups. The first subgroup was *impose costs on malicious actors*—in the form of penalties, criminal prosecution, or even retaliation. These are activities that increase the potential negative consequences for actors engaged in malicious activities. The second subgroup was *deny benefits to malicious actors*. This included making systems more difficult to penetrate (perhaps by raising security standards) and removing the incentive or reward for the activity (perhaps by encrypting credit card information to reduce the value of data breaches or by rapidly canceling accounts to reduce the value of stolen credit cards). These activities serve to defend systems and—to the extent that these actions are perceived as consequential by a malicious actor—they also serve to deter malicious activities.[3]
- **Protect values and benefits.** This perspective strives to protect civil liberties and individual privacy while allowing users to continue reaping the benefits of access to information and ideas, collaboration opportunities, and high-speed capabilities. Security

[3] Note that even publicizing defense or cost-imposition strategies (even if they are not actually implemented) may have a deterrent value if doing so influences a malicious cyber actor's perception.

features that bog down cyberspace to the point of limiting financial transactions, inhibiting data sharing or streaming, or preventing systems from functioning properly would not be compatible with this goal.

- **Create and foster innovation.** This perspective prioritizes continued innovation and development as the key to solving cybersecurity problems. It therefore works to ensure that innovation continues and that there are strong economic incentives for companies to invest in new ideas. This perspective generally opposes cybersecurity policies that cause economic harm to the IT sector or policies that constrain technological solutions to cybersecurity challenges (for example, standards mandating specific cybersecurity approaches).

We divided these three overarching themes into a total of six perspectives, as shown in Table 3.2. Figure 3.1 shows the relationships among the six perspectives.

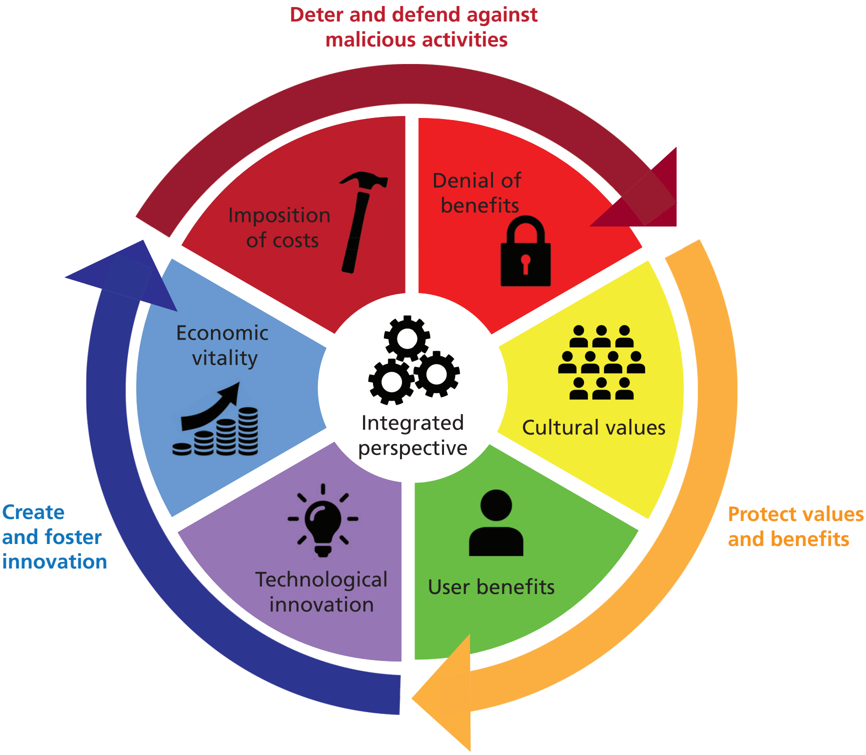
After the six teams were assigned, the game's senior official tasked players to define the underlying nature of the problem presented in the scenario; determine pivotal stakeholders involved, along with their equities and relationships; examine competing societal interests; and identify potential solutions to effectively navigate the resulting incentives and impediments.

Each team was designed to be multidisciplinary and included participants from each of the ten categories of ecosystem stakeholders. Thus, each team had participants with significant executive, legislative, legal, economic, technology, policy, security, and privacy expertise. At the same time, imposing a particular perspective on each team forced most players—perhaps for the first time—to look at cybersecurity challenges from a perspective that was not naturally theirs. For example, law enforcement officials who were assigned to the cultural values team had to look at the cybersecurity challenge from the viewpoint of civil liberties and freedom of information. National security officials had to prioritize the economic and business consequences of potential cybersecurity policies. Likewise, civil libertarians had to identify policies to strengthen law enforcement and prosecution of malicious cyber actors.

Table 3.2
Overarching Themes, Perspectives, and Assignments for Breakout Group Discussions

Overarching Theme	Specific Perspective Assigned to Teams	Assignment
Deter and defend against malicious activities	Impose costs on malicious actors	Encompasses efforts to penalize, prosecute, or otherwise impose consequences on malicious actors. Key issues include authorities, legal/civil remedies, law enforcement skills and capacity, and the deterrent value of such actions.
	Deny benefits to malicious actors	Encompasses efforts to ensure that malicious actors are denied success in exploiting potential targets. Key issues include standards, regulations, compliance mechanisms, technology solutions, and the deterrent value of such actions
Protect values and benefits	Protect cultural and societal values	Encompasses values that define society. For the purposes of our exercise, key issues included civil liberties, free markets, Internet freedom, adequate rule of law, and multistakeholder governance in cyberspace.
	Protect users' benefits in cyberspace	Encompasses efforts to ensure that society as a whole continues to experience the benefits of the IT revolution. Key issues are empowerment, productivity, overall utility (including the ability to transact commerce reliably), reliability, safety, and access to information.
Create and foster innovation	Promote technological innovation	Encompasses the environment that fuels the ongoing technological revolution. Key issues include maintaining an innovation-friendly environment, rules for sharing information, and promoting public and private research.
	Promote economic vitality	Encompasses considerations important to maintaining long-term U.S. economic interests and the global competitiveness of the IT sector.

Figure 3.1
Goals of Game Participants: Breakout Sessions



RAND *RR1700-3.1*

Game Play

Our cybersecurity-focused 360° Discovery Game began with a plenary session in which we presented the full group of players with the first of two scenarios via an immersive audio-visual presentation. The players were then divided into multidisciplinary breakout teams based on the perspectives discussed earlier and asked to address the challenge from their assigned perspective, but also according to their own specific real-world experience and expertise. Over the course of the breakout team deliberations, players brainstormed solutions, root causes, key stakeholders, equities, incentives, and impediments to solutions.

At the conclusion, the breakout teams came back together for a second plenary session, during which each team presented its findings. The senior official moderated the discussion and challenged the breakout groups to address the following questions:

- How would they increase the cost of malicious activity enough to deter bad actors in the scenario presented?
- How would they sufficiently deny the benefits of malicious activity to deter bad actors?
- How would they protect the values that are most important to society from bad actors and measures against these actors?
- How would they ensure that user benefits outweigh costs when participating in the connected world?
- How would they sustain technological innovation and leverage it to overcome the cybersecurity challenges?
- How would they sustain the IT sector's economic vitality and leverage it to overcome the cybersecurity challenges?
- How would they address the cybersecurity challenges of the scenario in a balanced manner?

The process was then repeated for the second scenario, with players assigned to different breakout teams to foster additional relationship building and exposure to new ideas.

Analysis

Note-takers kept a detailed record, in accordance with the Chatham House Rule, of players' game discussions, idea generation, and identification of challenges and hurdles. The RAND team analyzed these notes to identify areas of agreement and disagreement and how different players' roles and real-world perspectives and experiences influenced the cyber ecosystem and the ability to implement solutions. We then used this analysis to develop our preliminary thinking regarding a framework for addressing cybersecurity challenges that spanned the range of stakeholder priorities. Our analysis highlighted opportunities for policy development, partnerships, and investment to navigate this complex ecosystem.

CHAPTER FOUR

Washington Beltway Game

RAND held its first cybersecurity exercise in its Washington, D.C., office on August 30, 2015. In this exercise, the two realistic, but fictional, scenarios had resulted in a crisis that the White House had decided to address head-on. To do so, the White House convened a task force of experts from across cyber disciplines—represented by the players—to provide the newly elected President with recommendations. In the Washington, D.C., exercise, the White House Chief of Staff, role-played by former Secretary of the Navy Richard Danzig, officiated the game and challenged the players to develop solutions to the two scenarios presented.

Players

The Washington game included 62 participants from across the executive and legislative branches of government (22 players), think tanks and academia (19 players),[1] IT producers and IT security companies (eight players), media and journalism (five players), advocacy organizations (four players), the financial sector (one player), and orthogonal thinkers (three players). The game was conducted under the Chatham House Rule, precluding us from identifying specific individuals. A

[1] Including personnel from U.S. national laboratories.

composite list of the organizations that sent representatives to the two games can be found in the appendix.

The executive branch government participants mostly represented national and homeland security and law enforcement agencies, with a few additional participants representing government equities outside of security, such as civil liberties and cyber oversight. Players from think tanks represented most of the major Washington-area think tanks doing work on cyber issues, with counterparts from academia who tackle these issues at the nation's leading universities. IT-sector participants represented a diverse set of interests, including major Internet companies, top-tier major developers of cyber infrastructure, and elite firms operating at the forefront of the cybersecurity sector. Participants from the advocacy field represented the privacy interests of individual users and civil liberties in cyberspace at leading nonprofit organizations. Players in the public face category represented a combination of recognized brands in cyber journalism and government-political journalism. The economic sector was represented by a player from a major financial institution.

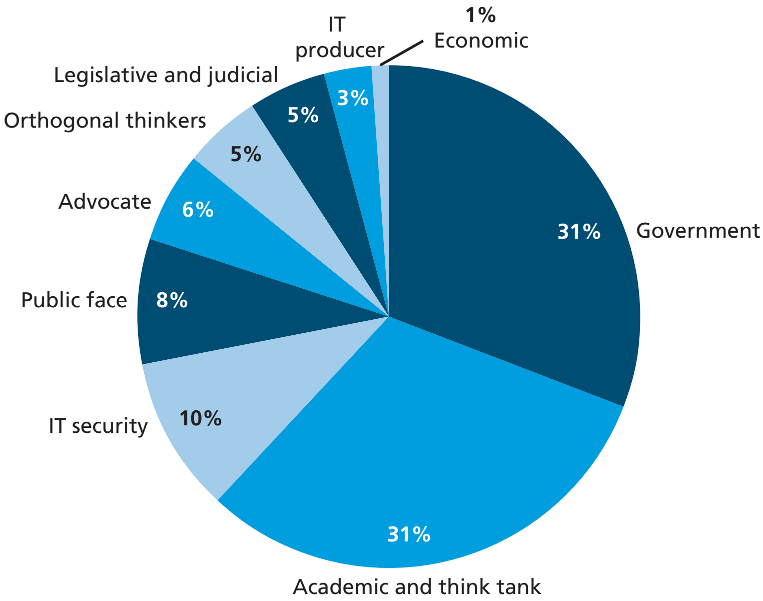
Together, the players represented a who's-who of U.S. cybersecurity discourse. The composition of the group is shown in Figure 4.1.

Scenario 1

This scenario led to many technology-focused responses and recommendations. Participants saw Internet Protocol version 6 (IPv6) as an improvement over baseline security for devices, simply through its increase in possible secure connections. Several participants suggested expanding the federal Managed Trusted Internet Protocol Service (MTIPS) and EINSTEIN intrusion detection system.[2] A simple solution suggested by two separate teams was switching the default setting of devices' Internet connections to "off." Many groups also agreed that

[2] The MTIPS program was developed by the U.S. General Services Administration to provide Trusted Internet Connections–compliant managed security services. EINSTEIN was created by the U.S. Department of Homeland Security to establish a common security baseline across the federal executive branch and to help agencies manage cyber risk.

Figure 4.1
Washington Beltway Game Participants



RAND *RR1700-4.1*

a major barrier to securing devices is the end user's failure to install patches and upgrades. This is a general problem throughout the cyber ecosystem, but it is a particularly serious one for IoT devices because they are often not easy to patch. In fact, there are IoT devices that cannot be patched at all, either because needed patches are not available (the manufacturer may have gone out of business) or because some IoT devices—mostly older devices—were not designed to be patched. This significant population of IoT devices that suffers known vulnerabilities but cannot be patched created a particular challenge for players as they deliberated the IoT scenario. As a possible solution to this problem, one group suggested encouraging a trade-in program, similar to the national "cash for clunkers" program for cars. Just as the cash for clunkers program incentivized owners to get rid of old (often highly polluting) cars in favor of newer cars, the IoT trade-in program would incentivize people to get rid of older IoT devices that cannot be patched or upgraded in favor of newer devices with better security and patching mechanisms.

Players suggested expanding existing federal initiatives, creating a "cash for clunkers" trade-in program for old devices, developing new national security standards, and assigning liability.

Participants also identified several legal approaches to promote better security through both patching and more secure designs. Government participation played a heavy role in these suggestions, which included incentivizing—or even requiring—upgrades of devices. An industry suggestion involved various possible mechanisms for requiring adherence to standards established by NIST as a consumer protection measure, or at least as a way for insurance companies to evaluate devices and allow actuarial rates to reflect how well an organization complies with such standards. (For example, companies that use devices that comply with standards would get lower rates, as would companies that install approved fire detection and suppression systems.) This led to questions about who would be liable in the event of a device failure, how to insure those devices or their users, and whether the current liability structure creates the right incentives for the market to reward security. The question of who pays was raised by nearly every team.

Hacking back was a popular solution—though no one established exactly what "hacking back" entailed or how it might work to reduce crime in the scenario.

Rather than simply legislating or insuring devices, some teams suggested a more aggressive and perhaps unrealistic approach. This included informing foreign governments that they need to control organized crime and that attacks on the IoT may qualify as unfair trade practice or even an act of war.

Likewise, "hacking back" was a popular solution—though none of the groups established exactly what hacking back entailed or how it might work to reduce crime in the first scenario. Private involvement in the investigation and securing of devices potentially offered the benefit of market competition driving more effective solutions, but it also evoked images of privateers on the high seas. Similarly, an open market in bounties to expose malicious actors could encourage aggressive white-hat investigations; without a mechanism to implement and disseminate fixes, it could also increase the attack options available to criminals. In this way, every solution brought further questions.

The expense associated with preserving IoT security and implementing potential solutions was a source of concern. Two teams reminded the collective that the costs already exist; these costs are just being ignored in favor of artificially inexpensive devices.[3] Several other teams pointed out that finding problems is a great first step, but fixing them requires personnel and time, which may not be available universally. Other approaches discussed included

- Internet service providers or third parties offering services to scan and filter Internet traffic for malware or patterns of malicious activity
- third parties offering maintenance of devices, including security updates
- private-sector investigation of cyber crime under a construct that the evidence collected could be turned over and used by law enforcement to prosecute cases.

Participants concluded that the decision to connect to the Internet matters, and the ability to update devices matters. Market forces might determine what different devices will do. The root failure is the tendency to not update, whether it is consumer failure or a failure of the supplier to generate updates. Both are problematic.

[3] As discussed in Chapter Two, the fundamental value that users seek from IoT devices (and cyber systems more generally) prioritizes performance, capability, and cost over security. Although users want cybersecurity, they are not yet willing to pay for it by prioritizing security in the marketplace or by practicing cyber hygiene to make up for this shortfall. Thus, we see the proliferation of a variety of IoT systems with little or no cybersecurity designed into them.

There was broad recognition of the power of market forces to drive improved security. Participants considered the private sector more likely to develop the expertise and capacity needed to scan Internet traffic for malware or to conduct investigations against criminals who threatened the IoT. They believed the government was unlikely to ever have sufficient capacity or expertise capability to effectively deal with the underlying problems. They saw market competition as likely to drive the continuous improvement of security practices and products. Government approaches, participants concluded, were likely to institutionalize security practices that would become obsolete quickly. However, there was no clear vision for how to harness this market power, nor was there an understanding of what incentives might be used to drive market behavior.

Scenario 2

In this scenario, attacks on major retailers, government systems, and insurance companies have led to massive database breaches. Malicious actors have also stolen a state's entire driver and vehicle registration databases. Criminals have used the data to generate high-quality counterfeit licenses (often in the name of a legitimate individual), resulting in a tremendous increase in the volume and cost of financial crimes. Furthermore, the compromise of drivers' licenses, combined with leaked government access data and the easy availability of high-quality forgeries of foundational documents, such as licenses and birth certificates, has compromised the integrity of other U.S. identity documents. Fraudulent birth certificates and licenses (potentially carrying the name of legitimate individuals but exploited by a malicious actor) can be used to obtain government credentials, such as passports or even U.S. Department of Defense–issued Common Access Cards (CACs). The increasing numbers of forged or fraudulently obtained passports raises the risk that unauthorized individuals will gain entry into the United States. Similarly, the rise of either forged CACs or CACs obtained based on fraudulent documents has put at risk the effectiveness of access control at sensitive military facilities.

Participants noted a series of vulnerabilities in the status quo. Leading problems included the amount of data that people are obligated to share to identify themselves, including date of birth, Social Security number, zip code, phone number, mother's maiden name, favorite pet, and even biometrics. Agencies at the state and national levels have different standards and procedures for securing user information. When acquiring identity documents, originators rarely enforce checks as strictly as they should.

Players identified several ways to mitigate the risk of identity theft, however. For example, they suggested creating a completely public document that serves as a "block chain" for an individual, summarizing all transactions and information in the spirit of public transparency. A national identity card came up several times in more than half of the groups. However, participants recognized civil liberties concerns and the danger of putting "all of one's ID eggs in one basket." Multiple forms of authentication (e.g., chip and pin, token, password) serve as a simple way to improve authentication protocols, as do multifactor authentication schemes. Each team noted that biometrics could improve authentication, but this is not a perfect solution, because biometric credentials cannot be replaced once they are compromised. Participants also cited secure information storage as a significant problem. Solutions included limiting insurance to companies that store account information in a secure manner. Players saw human confirmation of another user's identity as a strong form of identification. A simple but radical solution that the teams suggested was setting credit files to "freeze" by default rather than requiring users to request a freeze on their credit and renew it every three months. These forms of mitigation would require different levels of effort from users and companies.

Players suggested creating personal block chains, a national identity card, human confirmation for other users, and freezing credit every three months until verification is received.

Risk need not be the same under all circumstances or for all transactions: After all, buying a car with no money down is different from buying a soft drink with a credit card, and the transactions probably do not deserve the same level of verification. Similarly, different levels of verification provide different degrees of risk at different costs. More stringent protocols and, thus, lower risk may mean a lower insurance premium, for example. Balancing cost against consequences makes it only natural to consider implementing higher security standards only for "larger" transactions. While the idea of tailoring the degree of verification to the "size" of the transaction is attractive, the participants were not clear (nor always in agreement) about the risks or what "large" meant in this context.

Players argued that society fails to differentiate between identification and authentication.

Players argued that society fails to differentiate between *identification* and *authentication*. Identification is simply declaring one's identity, whereas authentication involves verifying that the claim is accurate. Correctly making this distinction suggests the need for a different mechanism for verifying the age of a person entering a bar than for confirming who is boarding an airplane. Likewise, not all authentication protocols are the same: A car purchase does not require the same level of authentication as purchasing a cup of coffee or entering a bar. Ideally, only the information that is relevant to a particular transaction will be exchanged as part of the authentication process. Rather than needing to know the birthdate and address of a person entering a bar, the bar only needs to verify that the customer is over 21. Rather than unequivocally identifying users, there is merely a need ascertain their right to access.

Participants discussed whether private-sector identification and authentication schemes should replace government identification documents for private-sector transactions (e.g., Social Security numbers, drivers' licenses, birth certificates). This appealed to many participants because market competition would drive improvement. Participants also argued that market options were a way to address privacy and civil liberties issues, as users could make individual choices to balance their concerns about risk and their desire for privacy.

Much like in the first scenario, there was a desire to hit back. Participants suggested internationally sanctioning bad actors or threatening the economies of their home states. This might include withholding trade or instituting political sanctions. Some participants suggested a privateer-like system in which the U.S. government authorizes certain private groups—under specific circumstances and rules—to not only trace and collect evidence against criminals but perhaps even to attack criminals via cyber means (e.g., rendering stolen material found on a criminal's systems inaccessible by deleting it or disabling the storage media) without fear of prosecution.

Participants concluded that the identity fraud problem may be easier to address than the IoT problem: Various forms of technology for improved identity verification and authentication are already available and could be deployed centrally (e.g., via financial institutions' websites). In contrast, the IoT landscape consists of myriad widely dispersed systems, many with very limited capabilities: It may be hard to both implement needed security mechanisms and distribute them to end users' devices. The main barrier is a lack of will to change the status quo and uncertainty about the adversary. The current legal solutions place all responsibility on the victim to deal with the fallout of fraud, which prevents appropriate incentives for market forces to address this problem.

Themes and Conclusions from the Washington Beltway Game

Both scenarios presented conflicts between maintaining rule of law and civil liberties during a national security crisis that taxes the limits of the U.S. government. The exercise presented players with fundamental questions about who is responsible for cybersecurity. Not surprisingly, each of the breakout teams generally proposed very different solutions based on their assigned functional orientation. While not evident in the teams' proposed solutions, integrating all perspectives revealed three broad themes in the conclusions from the Washington, D.C., game:

- **Deference to government solutions, due to the government's ability to rapidly generate unity of effort in a crisis.** The high percentage of players with government experience and memories of the recent debt crisis appeared to contribute to this perspective.
- **Desire to create marketplace solutions, because they will naturally reflect user equities.** Most teams explored some version of "security as a service" to compensate for shortfalls in capacity and expertise in the public sector, to drive improved security via market competition, or to address privacy and civil liberties issues.
- **Desire to create market incentives for cybersecurity.** Teams questioned whether companies are incentivized in a way that promotes cybersecurity, and they debated ways to create such incentives.

Washington, D.C., game participation skewed toward U.S. government roles and was lighter on parallel experience in technology, entrepreneurship, and corporate operations. Furthermore, the scenarios placed participants on an interdisciplinary panel advising the White House on cybersecurity policies. These factors likely contributed to the direction of the teams' discussions, with the majority of proposed solutions focused on direct government action in the form of regulations, setting and enforcing government standards, or legislative initiatives to strengthen law enforcement on cybersecurity issues. While few teams formally proposed solutions that harnessed market forces or incentivized private-sector action, in their internal discussions, most teams explored market-based solutions via some form of security as a service.

Breakout team discussions also generally considered whether market forces provide the appropriate incentives to drive cybersecurity. Participants pointed out that, in many cases, responsibility for cybersecurity lies with a party other than the one that incurs risk from breaches, leading to misaligned security priorities and imbalanced incentives. They discussed who would be liable when devices become compromised and damages occur. Should liability be shared by the device manufacturer, the software developer, and the seller of the device? Or is the user liable for whatever risks come with accepting the license agreement and deciding to use the device? While the answers to these questions will create incentives or disincentives to improving cybersecurity, it was not immediately clear to participants what the best approach would be.

This initial cybersecurity exercise generated informative discussions and provided some insights into how the various aspects of the larger cybersecurity problem interact. Because exercises tend to have their own idiosyncrasies, depending on the participant mix and the interactive chemistry within groups, no single exercise will fully illuminate a given challenge. As such, it is important to develop a statistically viable series of such exercises. Due to the heavy government representation in our initial exercise, we incorporated lessons learned and created a second exercise, which we held in a setting that was likely to better capture the perspectives of technologists, entrepreneurs, and the broader private sector, as described in the next chapter. In subsequent games, we will explore a broadened set of civil liberties and privacy issues associated with cybersecurity, drawing on a wider and more diverse set of participants.

CHAPTER FIVE

Silicon Valley Game

RAND held its second cybersecurity exercise at the University of California, Berkeley, on April 18, 2016. This second exercise was designed to better explore nongovernment approaches to the two cybersecurity scenarios. That was the primary reason for holding it in the Silicon Valley area. To further encourage nongovernmental options, we presented the two scenarios in the context of the private sector trying to preempt potentially ill-advised government actions. In this exercise, a fictitious, nonpartisan, cyber-focused think tank had convened a task force of experts from across cyber disciplines—represented by the players—to provide recommendations for dealing with the developing cybersecurity crises. Justice Mariano-Florentino ("Tino") Cuéllar, playing the role of the think tank's director, challenged the game's players to develop solutions to the crises presented in each scenario.

Players

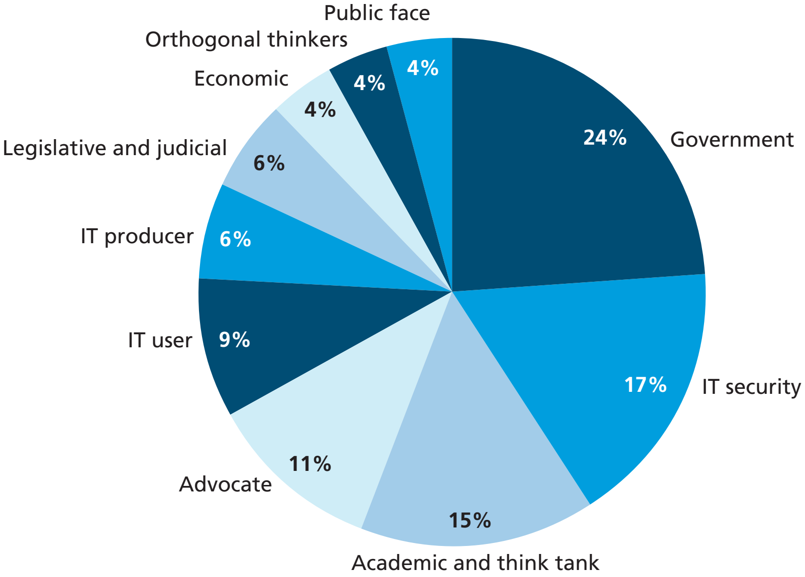
The Silicon Valley game included 47 participants representing IT producers, IT users, and IT security companies (15 players), federal and California state government agencies (14 players), think tanks and academia (seven players),[1] advocacy organizations (five players), media and journalism (two players), the financial sector (two players), and

[1] Including personnel from U.S. national laboratories.

orthogonal thinkers (two players). The game was conducted under the Chatham House Rule, which precludes us from identifying specific individuals. The composition of the Silicon Valley group is shown in Figure 5.1. A composite list of the organizations that sent representatives to the two games can be found in the appendix.

The game's location adjacent to Silicon Valley attracted participants from think tanks and universities in that region who might not have traveled to an East Coast event. Private-sector participants included the type of leading software and cybersecurity companies that one might expect, along with representatives from Fortune 500 companies. From the federal government, the game included participants from multiple U.S. Department of Energy national laboratories, along with other agencies' Silicon Valley field offices. The game also included representatives from two different state-level agencies. Similar to the Washington game, the Silicon Valley exercise included advocacy

Figure 5.1
Silicon Valley Game Participants



RAND *RR1700-5.1*

organizations representing privacy interests and civil liberties in cyberspace, as well as media organizations from both traditional publications and "new media" sources.

Scenario 1

In this scenario, similar to the Beltway game, participants confronted a situation in which the IoT has been overrun with criminals who profit from users, creating backlash within the IT sector. Participants felt that one of the key challenges was to support the development of the IoT and disrupt the criminal business model without adversely affecting society. Their goal was an IoT infrastructure based on protection, safety, and trust.

Across the breakout groups, players searched for a framework—or structured model—that balanced the security of the ecosystem (in the form of regulation, law enforcement, and data sharing) with private-sector goals (i.e., innovation, profits, and time to market). Discussions focused on the search for this balance and, specifically, a structure to capture it.

Across the breakout groups, players also described seeking a balance between risk management and rules for liability against market incentives and not overregulating. This balance was described as greatly needed, but no group could describe what it would look like. Key discussion points included the following:

- **Risk management.** There is a need to define risk and identify what is an acceptable level of risk for the individual and the masses.
- **Liability rules and pressures.** There is a need for liability rules that do not have a chilling effect on the economy. Approaches included imposing caps or limits while incentivizing good activities.
- **Market incentives and market pressures.** There is a need for rewards or incentives for both producers and purchasers (whether

individuals or organizations) to increase security, safety, and data sharing.

- **Regulatory pressures.** Regulatory mechanisms should incentivize good practices without stifling progress.

Players described the benefits of increased data sharing of security risks and vulnerabilities but were concerned about how such practices could compromise the inherent value of a product. For example, they discussed the risks associated with someone hacking an autonomous vehicle, potentially leading to a loss of life. However, they did not want to give up the inherent benefits of autonomy—the societal and economic benefits of reduced collisions and new designs for transportation infrastructure—by requiring systems that users could override.

Another example of this balance between benefits and security risks was discussed in terms of the lower-cost IoT devices on the market that make a profit primarily by selling information collected from their users. This information is generally sold in aggregate or anonymized form, and users can rarely control how it is sold and to whom. Participants advocated for rules around data sharing to allow users to opt out and to remove incentive structures for business models that profit from sharing users' data, but they realized that some information sharing—even for revenue-generating purposes—should be allowed. The groups did not fully address this contradiction.

Discussions about information sharing focused on the need to reveal and share information about security vulnerabilities, as well as creating incentive structures and requirements that facilitate transparency around security. Participants argued that increased transparency regarding vulnerabilities and patch availability for IoT devices would encourage competitive pressures to provide software updates and ensure maintenance of devices, as well as facilitate the auditing of fundamental security systems. Players also believed that

Players described seeking a balance between risk management and rules for liability against market incentives and not overregulating.

the wide availability of such information would encourage (or perhaps pressure) the industry to develop and promote a system of self-regulation and best practices. While participants were less decided on how often to provide updates, they agreed that greater transparency would foster the creation of needed trust networks. They felt that regulations could be put in place to further enforce such transparency and data sharing but must be designed in a way that protects privacy and promotes security. A related idea put forward by participants was to develop incentives for testing and improving security features, as well as removing impediments to cybersecurity research.

Players revealed their preference for different rules for devices that could cause physical harm and death and for those that cannot. They believed that rules and regulations should vary based on the potential damage an affected device could inflict.

Throughout the conversations, players revealed their preference for a system that provides different rules for devices that could cause physical harm and death (e.g., autonomous cars) and for those that cannot. They did not believe in a one-size-fits-all approach; rather, they concluded that rules and regulations should vary based on the potential damage an affected device could inflict.

While they discussed challenges in retroactively introducing security into a system with unsecure underpinnings, the players were fairly optimistic about the possibility of resolving this challenge.

Meanwhile, in one group, players recognized that these technologies are global and believed that it would be difficult to create and enforce laws across all borders. Instead, they proposed developing norms of behavior that would describe socially acceptable and unacceptable behaviors regarding IoT products and their use. There was no clear view as to how such behaviors would be defined or how to motivate adherence to agreed-upon norms. Some participants also viewed law enforcement as woefully behind both the technology and criminals. They also discussed the inherent lack of jurisdictions in cyberspace as a challenge for prosecuting criminals who exploit IoT devices and the need for better law enforcement tools to collect evidence, identify perpetrators, and prosecute them. This applies to jurisdictional questions across local, state, and federal levels within the United States and to international jurisdictional considerations. Today's tools require law enforcement officers to become IT experts. Players emphasized that what is needed is something analogous to the breathalyzer, which law enforcement officers can use easily to reliably identify intoxicated drivers without having to understand the underlying chemistry.

The group was divided between players who believed in free-market dynamics and had faith that the market could correct itself and those who wanted some degree of regulation. For example, some players suggested that the government could influence the market indirectly by establishing purchasing standards for its own systems, which could then influence industry decisions in prioritizing more secure devices.

For free-market thinkers, user choice was described as the most effective tool, but this requires both motivating users to care about security and providing information to enable rational decisions, such as labels regarding security features or universally understood seals of approval, as well as education about cybersecurity. Players thought information could be provided by a combination of private-sector standards and government requirements for meeting or reporting that information to consumers.

Players believed government has a role in cybersecurity education, yet there was strong disagreement as to what constituted good cybersecurity education and how it should be provided.

Many groups discussed education as a necessary tool to raise consumers' and users' awareness of cybersecurity issues and the consequences of poor security decisions, as well as to inform them of their choices and enable rational decisions. Players believed that the government has a role in cybersecurity education—either through public education and awareness campaigns or by requiring such information to be included in school curricula. However, there was strong disagreement as to what constituted good cybersecurity education and how it should be provided. Players believed that the government should raise awareness and educate the public about the potential benefits, costs, and risks of different technologies, such as by issuing a government report investigating high-profile incidents.

By the end of the game, two key questions that had been raised by the groups remained unanswered and are candidates for future study:

- How can companies be incentivized to share information about their devices' vulnerabilities and patch these problems without jeopardizing individuals' privacy?
- How can individuals accurately assess costs, risks, and benefits, especially when risks may be determined by others' choices and an individual's understanding of consequences is generally poor?

Scenario 2

Sharing the fundamental ingredients with the second scenario in the Beltway game, Silicon Valley players in each of the breakout groups described the need to protect the global financial system from collapse or paralysis, with *paralysis* defined as the inability to execute transactions on a mass scale because the authenticity of the transaction—the sender, the recipient, or the broker—cannot be validated. The damage was compounded as the inability to execute transactions caused cascading problems. (For example, the inability of financial institutions to process automated paycheck deposits made it impossible for individuals to make mortgage payments, pay other bills, or withdraw cash, leading to immediate physical and financial consequences and long-term inconvenience for consumers.) Players discussed mechanisms for users to selectively freeze accounts or transactions; for institutions to identify, quarantine, and repair damage; and for institutions or individuals who suffered consequences to pursue damages from parties deemed at fault (e.g., the party or parties responsible for depositing the paycheck).

One of the major challenges to this end state is the need for attribution—the identification and verification—of adversaries so they can be punished and future adversaries can be deterred. Participants acknowledged that this becomes complicated when state sponsors are involved. Players suggested international agreements, such as mutual legal assistance treaties,[2] and the possibility of enlisting and certifying "bounty hunters" to identify bad actors and report them (along with supporting evidence) to companies or law enforcement. While the groups raised the issue of what could be done with incomplete or imperfect attribution, the discussions did not explore this possibility.

Within the financial system, multiple breakout groups independently described the ability to electronically watermark e-money or use a block chain to improve the ability to track transactions, though players acknowledged that doing so may reduce consumer privacy.

To pay for the development of new capabilities (whether better law enforcement, tools to determine attribution, or new identification and authentication schemes), players suggested a transaction tax on Internet connections to support research grants (directed by the government) and the development of digital renaissance zones. These zones—which could be geographic or virtual—would target digital businesses (particularly cybersecurity businesses) with incentives to foster innovation and to promote cleanup and cyber hygiene. They also proposed a liability regime with a new, stronger identity management system; users who work with the stronger identity management system could be given certain liability protections (within appropriate constraints and limitations) when breaches of anonymity or security occurred.

As with a true financial crisis, the players had difficulty focusing on long-term solutions versus immediate reactions to prevent further economic collapse. The players acknowledged that an economic crisis may not be averted, but actions could be taken to mitigate how bad the situation gets. The group proposed stopgap solutions to help individual users while banks were closed in the scenario, including government-

[2] A mutual legal assistance treaty (commonly known as an "MLAT") is an agreement between two or more countries for the purpose of gathering and exchanging information to enforce public or criminal laws. They are negotiated by the U.S. Department of State in cooperation with the U.S. Department of Justice to facilitate international cooperation in criminal matters. Note that it is unclear how such a treaty would function if the target of the investigation were a state actor.

issued downloadable, printable IOUs insured up to a limited amount and recognizing those who help others during the crisis.[3] (Players imagined that eBay, for example, could modify its structure so that listings could be sorted by zip code to help people locate and perhaps trade for items that are immediately needed until normal commerce resumes.) They asked whether rollback mechanisms should be embedded within the cyber infrastructure itself.

Finally, the players questioned how users would establish new digital identities during or after a financial crisis. Any such process they could envision would require extensive review of documents and the "biography" of personal transactions. They imagined a more extreme version of the question, "What are the last five places where you used your credit card?" In fact, players viewed the history of public- and private-sector transactions (e.g., renewing a driver's license, getting a mortgage, using credit cards) in combination with ID tokens (e.g., drivers' licenses, passports) as the ultimate mechanism for verifying identity. In this light, they saw a trade-off between a system with integrity in which identities are verified and one that prioritizes privacy and confidentiality.

Themes and Conclusions from the Silicon Valley Game

Silicon Valley players focused on developing options that protect the economic well-being of the IT sector and the economy overall. The IT sector has been described as the "golden goose" of the U.S. economy, and there is a national interest in protecting it. As a result, participants felt challenged to promote innovation and mitigate hurdles for businesses to thrive while protecting user security, privacy, and national infrastructures.

[3] The problem of securing downloadable IOUs from hackers was identified as a significant challenge with this idea, but it is illustrative of the wide range of stopgap measures considered.

During both games, the players identified several challenges to their stated goals:

- **A globalized world means that isolated solutions are not useful and legal restrictions end at the border.** Any solution must cross international borders, leading players to talk in terms of norms of behavior and "redlines,"[4] rather than regulatory changes or legislation.
- **Changes to policies, social norms, or infrastructure could take a decade to implement.** The complications of working across multiple cultures and jurisdictions, and the hurdles of replacing or upgrading legacy infrastructure, can delay solutions. Participants found this to be true for both cyber infrastructure, designed before security was a concern, and for non-cyber infrastructure that has been upgraded piecemeal over time, such as the financial sector.
- **Regulations will not keep pace with technology.** Regulations are often reactive to societal change, and the lag time in creating and passing a new regulation makes it difficult to address new challenges in a timely manner.
- **Within the United States, working across state governments magnifies challenges.** Each state would have its own approach, which may conflict with those of other states and with those of the federal government.
- **There will be costs associated with any changes, and it is unclear who should carry the financial burden.** Users do not routinely choose to pay more money for more secure capabilities, which is one reason that there are so many unsecure products in the marketplace. IT providers could lose profitability if they had to embed these costs into the devices and pass them on to buyers who do not value such features.

[4] By *redlines* we mean the furthest limits of what will be tolerated; that is, what are the hard limits beyond which a party will not go in a negotiation?

It was somewhat surprising that an exercise intentionally weighted (by location, attendees, and scenario setup) toward nongovernmental approaches still resulted in numerous discussions and suggestions involving government actions, such as regulation, incentives, and education mandates.[5] Although participants recognized the dangers and unintended consequences inherent in government interventions, they did not always believe that the market would naturally move in directions favoring cybersecurity without some government involvement. There was little clear agreement on what action the government should take or how to bring it about, however. There was also limited discussion of whether such interventions would actually achieve the desired effects. Such questions invite focused follow-on research, as discussed in Chapter Seven.

[5] This phenomenon could be a result of the game's design. It is feasible, though not validated by any observations during the game itself, that since the scenario presented a society in crisis, participants felt that subtle nongovernmental preventive solutions had failed, so they looked to direct, government-imposed solutions to deal with a crisis that could be perceived as cascading out of control.

CHAPTER SIX

Analysis of the Two Cybersecurity Games

In both games, participants focused on how to manage the risk and consequences of cybersecurity breaches. They saw the need for a public-private partnership as part of any framework for addressing core cybersecurity challenges, but there were fundamental differences in how they envisioned that partnership. Participants in the Washington game had generally bigger roles for government, for example arguing for designating elements of the IoT as critical infrastructure to encourage additional government-imposed protections and security measures to support the health and prosperity of the IoT over the long term. In contrast, Silicon Valley participants cautioned that government measures could become mandates that lock in suboptimal solutions and stifle the creation of new, innovative solutions. Silicon Valley players instead saw a need for fundamental changes in business models for the digital age, especially in models that use consumer information as a means for generating profit.

Throughout the games, the players' own perspectives influenced which topics were raised and in what context. When discussion turned to ideas for government regulations, oversight, or enforcement, the Washington participants were unable to agree on which government agency or agencies had the responsibility, appropriate authority, or capability to oversee the activity. In the Silicon Valley game, when a new regulation was proposed, it was discussed on its merits only, and questions of responsibilities and authorities were never raised.

When laptops are purchased for schools and spyware is installed to monitor student behaviors, whose privacy and civil rights should be protected: the school's or the student's?

When players talked about the need to protect the users' security, the Washington and Silicon Valley groups had different opinions about who constituted the "user." In Silicon Valley, players discussed the complexities that arise when the consumer is not the user, such as when laptops are purchased for schools and spyware is installed to monitor student behaviors. The players debated whether the user was the school, which purchased the laptops, or the students who actually use the laptops.[1] This, in turn, raised questions of whose security should be protected and what privacy meant in this context. In Washington, there was never any similar such discussion, and the players did not make distinctions between user and consumer.

This chapter highlights specific commonalities and differences in discussions of each scenario across the two games.

Scenario 1

This scenario revealed the need to assess the relative risk of IoT devices and treat higher-risk threats with greater scrutiny than lower-risk threats. If an IoT device that could lead to death—such as in the case of failure of a medical device or an autonomous vehicle—that device needs a higher level of security scrutiny than a device whose greatest threat is user inconvenience, such as a disabled toaster oven or alarm clock. (This would of course, require making *ex ante* assessments of which devices could cause what level of harm, as well as where there

[1] The topic of teaching children the importance of maintaining and respecting personal privacy while monitoring their behavior—and whether it was possible to do both simultaneously—led to a spirited debate.

might be unintended consequences arising from interconnected systems.) Players generally believed that the higher the risk tier, the more the government should play a regulatory role, and, at all risk levels, stakeholders in the cyber ecosystem should shape the marketplace and the government's role in accordance with the severity of the risk to their equities.

There was much discussion of the role of government in IoT oversight during both games, and the players identified the following as the key government roles:

- Develop cybersecurity standards, including standards for digital identification mechanisms or credentials.
- Implement a user's bill of rights, guaranteeing that consumers are informed about privacy and security behaviors and the implications of the devices and systems they use.
- Facilitate information sharing and security benchmarking between government and industry—and within these sectors—to facilitate action against vulnerabilities and exploits.
- Provide financial incentives for improved cybersecurity (for example, in the form of tax breaks).
- Direct research funding toward developing technologies and techniques to affordably and effectively comply with standards.
- Educate consumers, through either public awareness campaigns or school curricula.
- Develop a system of security labeling, similar to food nutrition labels, to allow consumers to easily compare technology products side by side.

Silicon Valley participants specifically called out the need to change the balance of power of EULAs, but they did not describe who—government, industry, or consumer advocacy groups—should drive that change.

Commonalities

Participants in both games identified a common set of challenges, saw a similar set of underlying causes, and framed the issues similarly. They saw the fundamental problem as vulnerabilities in the IoT systems driven by market forces that do not reward security and encourage the entry of non-software-savvy companies into the software market (e.g., refrigerator makers). Participants took the position that having market forces reward security was the only way to bring security to the IoT. Where the two games' participants differed was in how to engage market forces to drive security.

Both groups of participants envisioned a role for government, but the nature of this role differed. Washington participants, perhaps because many came from national security or law enforcement backgrounds, saw a government role in setting standards for security as a privately provided service and establishing regulations or processes to formally "deputize" security providers (in the sense of collecting evidence of cyber crimes that could be used for prosecution). Their idea was that when users contracted for Internet service, they would also have the option of contracting for an Internet security service (perhaps with a choice of several levels of service from different providers). This security service would monitor incoming and outgoing data streams for suspicious activity. If such activity were found, the service would warn the user and could block the activity. Going further, the participants suggested that the cybersecurity service could be certified to collect data and conduct forensics that would be accepted by law enforcement as evidence for possible prosecution of the guilty parties. In contrast, Silicon Valley participants saw the government's role as promulgating, requiring, or even enforcing standards that had been developed by industry via more traditional, collaborative processes.

Both groups saw a need for a government role and identified a potential solution in classifying products by degrees of cybersecurity. Ideas for doing so included creating an organization (loosely modeled on Underwriters Laboratories Inc.) that would endorse products based on their security testing or according to a government security rating system or having manufacturers self-certify their products according to universal standards. Participants in both games discussed a need for some kind of partnership of government and industry to implement such a system; Washington players emphasized testing and certification, whereas Silicon Valley players emphasized security performance standards. Participants in both games also saw a role for the government to create its own standards and buy only products that meet high standards, thus helping to drive the market toward a more secure IoT.[2]

Participants in both games saw some need to prioritize the cybersecurity of the IoT according to the impact of failure. Both groups identified health and safety devices as the most critical for regulation. Washington players preferred to assign liability to the producer of such critical IoT devices, however, while Silicon Valley players emphasized the need for a regulatory process modeled after commercial aircraft avionics certification to certify critical IoT devices.

Both groups of participants emphasized the need for penalties for attackers and improved investigatory approaches to ensure that malicious actors could be caught and punished. They considered this more important than penalties for the IoT producer. They also suggested incentives for producers. Neither Washington nor Silicon Valley participants discussed a larger role for the consumer, other than being given the knowledge of which software, devices, and platforms are more secure to encourage informed buying decisions. Washington participants noted that most crime-prevention approaches involve deterrence rather than making an attack impossible. Silicon Valley participants asserted that as long as there are financial benefits to an attack, deterrence will not be effective. (They cited harsh penalties for drug trafficking as a poor deterrent in stopping that illicit industry.)[3]

Participants in both games agreed that the technical competence for solving the problems outlined in the first scenario lies with industry, not the government, and that solutions need to come from government-industry collaboration. While both groups highlighted the potentially powerful role that market forces can play in security—and the large role that consumer choice could play in driving those market forces—neither group could see that happening without major actions by gov-

[2] This could be analogous to the minimal security requirements for federal information systems set by the Federal Information Processing Standards (see NIST, 2006).

[3] Note, however, that the appropriate way to measure the *deterrent* value of such penalties is not the absolute number of crimes but, rather, what the marginal increase in crimes *would be* in the absence of these penalties.

ernment, industry, or both to motivate consumers to choose better security and provide mechanisms to enable informed buying decisions. Neither group emphasized a significant role for the consumer in taking direct steps to better secure existing systems.

Differences

Washington participants focused on the challenges of implementing solutions and structural limits to a greater extent than the Silicon Valley participants. They deliberated such questions as which government agency would have regulatory oversight or write standards for products, how overlapping authorities could be resolved, how to avoid duplicating effort across agencies, and whether government agencies have the appropriate technical competence to perform this role. Silicon Valley participants brought up the challenge of writing standards—especially whether the industry would be able to avoid writing standards that advance its self-interests. However, they did not dwell on the topic to the degree that the Washington participants did, and they were not inclined to dismiss the idea of standards in light of this challenge.

Washington participants deliberated such questions as which agency would have regulatory oversight or write standards for which products, how overlapping authorities could be reconciled, and whether government agencies have the appropriate technical competence.

Washington participants identified a challenge in keeping an IoT device secure over its life cycle. They were concerned that manufacturers want to sell a product and move on and that they may stop offering security upgrades for older products or maintaining a necessary workforce to provide this support. They also noted that some products, especially early generations of home routers and home automation systems, have no means for security updates at all. These concerns were not raised during the Silicon Valley game.

Silicon Valley participants emphasized the relationship between the business model of IoT companies and corresponding security challenges. Business models that treat customer information as a liability were considered inherently more secure than other models, such as those that treat customer information as a means of generating profit. This perspective never came up in the Washington game, but in Silicon Valley it was considered one of the fundamental drivers of IoT insecurity. Silicon Valley participants identified liability and consumer education as two potential levers to influence companies' choice of business model, but there was no consensus on how to make use of these levers. There was also considerable skepticism regarding whether either could be used effectively.[4]

Silicon Valley participants discussed whether change could be achieved by having the government require better security standards for the IoT devices it purchases, but this idea never came up in the Washington game. The Silicon Valley group concluded that the government market alone was too small to drive change. This led to one idea for increasing the government's effective market share by mandating that all people with security clearances be restricted to buying IoT devices that meet government security standards. This was a pretty radical idea that raised questions about whether such a mandate was legal and whether cleared individuals (combined with direct government purchases) would have sufficient purchasing power to drive the market, and perhaps reflects an overestimation of the federal government's powers and economic influence by the Silicon Valley players.

The Silicon Valley game favored the idea that consumer choice could be used to drive the market toward better cybersecurity. However, in contrast to the Washington participants, the Silicon Valley group doubted the ability to empower consumer choice. Silicon Valley players identified two key obstacles to enabling consumer choice: the need for education and the unequal playing field created by EULAs. Neither of these issues was discussed in the Washington game. While there was near-unanimous agreement in both games that education was essential, there was no agreement on how to provide education, and there was general skepticism about the prospects of success. EULAs were

[4] For interesting perspectives on liability with regard to autonomous systems, see Beiker and Calo (2010), Roesner et al. (2014), and Calo (2016).

universally seen as inherently unfair in placing the security burden on the user, as the parties to a EULA have grossly unequal power.

EULAs were universally seen as placing the security burden on the user and inherently unfair, as the parties to a EULA have grossly unequal power.

Silicon Valley participants also stressed that user choice is not enough, because many IoT devices are not chosen by the user but by other organizations (such as schools or employers) that may make choices that do not prioritize user security. The classic example was school laptops that come with spyware preinstalled by the school system (for security and compliance purposes), and this spyware is usually not well protected from outside parties.

Washington participants strongly emphasized the need for better law enforcement, primarily through public-private partnerships and privatizing or deputizing industry to protect security functions. In the Silicon Valley game, better law enforcement was not seen as an effective way to address this problem due to criminals' advantage in needing only to seek out the weakest link.

Scenario 2

Washington and Silicon Valley participants did not define or frame the second scenario's challenges identically, perhaps due to differences in the scenario setup. Washington participants focused on nation-state threats and what constitutes personal identity. Silicon Valley participants focused on criminal threats, technologies, and incentives. Both groups discussed shortcomings in how the cyber ecosystem currently defines and verifies identity by using information that is frequently stolen and known to more people than just the user. When systems ask for more verification information—for example, in the form of personal security questions—it increases the probability that ever more specific data will be stolen and repurposed.

Commonalities

Participants in both the Washington and Silicon Valley games struggled to find a suitable solution to the loss of confidence in verifying identity. Players in both games decided that the entire system for establishing identity and authenticating transactions was fundamentally broken and headed in the wrong direction. They agreed that an underlying foundational flaw in the existing system is that it uses documents and credentials to verify online identity that were not created for this purpose, such as drivers' licenses, birth certificates, Social Security numbers, and birth dates. When this information is stolen, it cannot be changed. Participants agreed that overuse and overreliance on these data points for identity verification was a fundamental weakness of the current cybersecurity ecosystem.

Participants in both games highlighted the problem of credentials being overused for purposes beyond their intent. In both games, participants concluded that it would be best to develop a variety of identification mechanisms, tailored to specific purposes, overcoming this problem. Washington participants proposed specific ideas for doing so, while the Silicon Valley players did not.

Differences

Washington participants focused on the authentication problem and pushed private enterprise as a solution, with the idea of privatizing identification and authentication processes. In contrast, Silicon Valley participants focused on the breach problem and saw a significant imbalance of power between institutions that are breached and the individuals who suffer as a result of the breach. For this reason, they pushed for government regulations as a way to level the playing field between these two parties.

The principal difference between the two games was that the Washington participants saw privacy concerns as a major issue, whereas Silicon Valley participants barely mentioned privacy.

Washington participants also discussed what actions are involved in authenticating identity and whether too much personal information is often requested. For example, when purchasing alcohol, the only information a vendor needs is a customer's date of birth (or even merely confirmation that the customer is over the age of 21). The vendor does not need the person's name or address. Yet, too often, a liquor store will scan a customer's driver's license and store all the information on it. For more involved transactions, such as applying for a mortgage or a security clearance, a larger amount of personal information is needed. Discussions during the Washington game explored the idea of using a third party to verify users' identities for these complex transactions.

Specifically, Washington participants divided transactions into three categories:

- high-volume (e.g., buying a product online)
- high-value (e.g., an expensive purchase)
- high-security (e.g., a federal security clearance).

Washington participants felt that the first category was solely the responsibility of the market (within the context of existing consumer protection laws), and thus was not a topic relevant to the scenario, since they were to advise the government on policy directions.

Silicon Valley participants believed that patterns of behavior might be more useful than credentials for many transactions. They emphasized that passwords are generally not reliable and that many financial organizations already consider them compromised. Instead, they suggested challenging the authenticity of transactions that deviate from previous behavior. Players across breakout groups stated that increasingly sophisticated data analysis shows promise in using pattern analysis to limit identity theft, presumably drawing on recent experience with fraud prevention. Patterns could extend beyond transactional data to include data involving personal habits, movements, and other activities to create a complex pattern that would be difficult to spoof.

Silicon Valley participants believed that patterns might be more useful than credentials for many transactions. Such approaches challenge the authenticity of transactions that deviate from previous behavior.

Silicon Valley participants deliberated whether pattern analysis might also be used preemptively, to alert users that their identity was about to be stolen rather than merely detecting an infraction after the fact. The idea was to catch attackers rather than just protect the victims. The participants saw a role for government here but did not explore the potential privacy barriers.

Participants believed that Individuals should have a simple and free process to repair damage caused by a data breach.

Silicon Valley participants emphasized the need for an ability to "roll over" credentials (including associated histories) into new credentials, as is done when credit card numbers are changed after being compromised. They found the inability to roll over biometric credentials (people cannot be issued new biometrics) to be a limitation, but several participants still found biometrics a promising solution. The participants agreed that Social Security numbers are a poor credential because there is no process to roll over a compromised Social Security number and account into a new number when one's identity is stolen.

The Silicon Valley participants were more optimistic that current technologies can satisfactorily authenticate personal identity, but they pointed to barriers in consumer adoption. Several players cited multifactor authentication as an example of a technology that is not used as widely as it could be. They even explored the unsettling idea of a physically embedded public key infrastructure certificate assigned to everyone at birth. The discussion acknowledged social barriers, and participants concluded that the public was not yet scared enough to go to these lengths. They viewed current approaches as fairly secure but still saw a need to be able to roll over multifactor identification credentials if compromised.

Despite this optimism, or perhaps because of it, Silicon Valley participants thought that it was important for government to fund and support the development of effective standards for security and identification, as well as the development of affordable and effective technologies for implementing those standards.[5]

Perhaps due to the slight structural differences between the Washington and Silicon Valley games, Silicon Valley participants focused more on the institutions and relationships in this scenario than participants did in Washington. The Silicon Valley players also focused on financial institutions, which they perceived as instrumental to the problem of digital trust and far more powerful than individuals. This group raised three key suggestions:

1. **Require strong reporting requirements for all institutions that hold personal data.** This idea was similar to reporting rules under the Dodd-Frank reforms implemented in the wake of the 2007 financial crisis. Participants recommended requiring institutions that store personal data to report regularly (annually or quarterly) on their holdings. They suggested an aggregate public report and individual personal reports for each user whose data is held. Such a bill could include requirements that institutions delete, de-identify, or otherwise aggregate "old" data. While the players did not arrive at a definition of *personal data,* they generally considered relatively broad definitions that went well beyond traditional "personal identification information" to include, for example, purchase and transaction histories and geolocation data.[6]
2. **Individuals should have the ability to easily and selectively freeze and unfreeze certain types of financial transactions.** For example, an individual should be able to selectively freeze credit card applications, loan applications, or the opening of new bank accounts.[7]

[5] A new federal strategic plan for cybersecurity research and development was released in February 2016 (see National Science and Technology Council, 2016).

[6] For a deeper look at how individuals conceive of private information, see Schneier's *Data and Goliath* (2015) or Richards's *Intellectual Privacy* (2015).

[7] Credit-freezing mechanisms already exist, but they place the burden to act on the user. While users currently have the option of freezing new credit applications, the default setting is openness, and it is not possible for consumers to flexibly tailor their credit reporting

3. **Individuals should have a simple and free process to repair damage caused by a data breach.** Today, when identity information is stolen, individuals are often left to fend for themselves to repair the damage, and this can be costly and time-consuming. Participants felt that this puts an unfair burden on victims who had no responsibility for the breach instead of on the institutions who held the data.

The Silicon Valley players also suggested that financial institutions should have a "rollback" capability so that, whenever a major breach is discovered, they can return their data to a known valid state to ensure the integrity of the financial system. Players reported that Estonia put in place such a mechanism after suffering a series of cyberattacks. They contrasted the current environment in the United States with that in Estonia, which routinely prepares for a massive financial cyber attack by conducting rapid-recovery drills. Players imagined a requirement to stress-test financial institutions being part of Dodd-Frank–like legislation for cybersecurity.

freezes. Game participants also argued that the need to repeatedly freeze mortgage or loan applications is an unnecessary burden. See Federal Trade Commission (undated, 2014).

CHAPTER SEVEN

Areas for Future Research

This project succeeded in laying the foundation for a preliminary framework for cybersecurity and simultaneously revealing areas for additional study. The games provided a wealth of ideas, but these ideas—even the most promising ones—could not be fully developed in the context of the games. In fact, one of the most valuable outputs of a well-designed 360° game is identifying interesting questions for further analysis. This chapter takes the ideas generated by the games and highlights issues that are most deserving of further research and study.

Key Issues for Study

The majority of the ideas discussed during both games will be impossible to implement if the cyber policy community does not first take action in three key areas of generating credible information for future decisionmaking: developing a reasonable way to monetize cybersecurity risks, finding an acceptable assignment of accountability and liability in the cyber ecosystem, and selecting, aligning, and empowering jurisdictions to enforce accountability and liability. These gaps prevent meaningful progress on cybersecurity policy. Players often assumed—explicitly or implicitly—that these goals could be achieved, yet none of the groups proposed viable solutions. Therefore, we propose the following future analytic efforts.

Develop an Approach to Monetize Cybersecurity Risks

Creating mechanisms for monetizing cybersecurity risks will inform existing cyber insurance markets and allow individual and corporate consumers to compare risks when buying new cyber capabilities. Finding an acceptable way to quantify and monetize cybersecurity risk will require collecting and analyzing data on cyber breaches, financial losses, and nonfinancial losses to methodically analyze what is compromised during a cyber breach, at what rates, who is penalized, and with what financial and nonfinancial costs.

Develop an Acceptable Assignment of Accountability and Liability

When risk is monetized, the next question becomes who should be responsible for the costs, both financial and nonfinancial. There is little consistency in how and to what extent accountability and liability are determined when cyber breaches expose an individual's medical records or compromise an individual's credit. Equally murky is liability in the case of harm caused by a malicious hacker who exploits an IoT device with inadequate security. Developing acceptable liability rules would require building on efforts to monetize cybersecurity risk by also collecting and analyzing cause-and-effect data, as well as by assessing the acceptable distribution of benefits and costs, as judged by a critical mass of the ecosystem in various loss situations.

Identify an Adequate Alignment of Cyber Jurisdictions

Jurisdiction over cyber events is obviously ill defined when malicious individuals in one country can attack individuals in a second country using hardware located in a third country. But even simpler cases, such as ransomware attacks or cyber extortion of individuals and small businesses, raise jurisdictional questions among local, state, and federal authorities, as well as international questions. Governments need sufficient clarity on jurisdictional questions to enable effective enforcement of acceptable cyber behaviors, liability, and accountability. Developing appropriate jurisdictional rules requires collecting suitable data on stakeholder effectiveness and public accountability, case studies on existing arrangements, and social contract research regarding which organizations would be acceptable to a critical mass of the cyber ecosystem. Using this information, qualified decisionmakers should determine which agencies and organizations have the authority to adjudicate and enforce accountability for losses or penalties for breaking norms of acceptable behavior.

Additional Topics for Study

Participants shared many ideas and proposals that raised questions amenable to further analysis. It is worth studying how the following ideas might be implemented, their effectiveness, and their implications.

The Concept of Tiered Risk

Players coalesced around the notion that all risks are not equal and that more threatening risks—those with the most damning consequences—should be treated differently from less threatening risks, which they called "nuisances." A high-risk threat may lead to loss of life, while the consequences from a low-risk threat or nuisance may be limited to user inconvenience. Possible topics for future research include how to define risk tiers in a useful way, determining the right number of tiers, and examining what types of actions or risk mitigations should be taken (and by whom) at each tier level, across different contexts.

The Role for Government in Cybersecurity

Players identified several opportunities for government action, each of which warrants further study, discussion, and analysis.

Government Purchasing Standards

Players believed that if the government sets minimum requirements for the security of the cyber capabilities that it purchases, then those requirements will filter down to consumer markets, both because the products will already be in manufacturing pipelines and because consumers will expect the same minimum security as government entities. Research is needed to test whether this "trickle-down" assumption is valid. If analysis shows that government purchasing standards can actually influence the larger market, further research would inform such standards. There is also a need for research on the overall efficacy of government security standards for IT, as the U.S. government's track record in this area is mixed.[1]

A Cyber User's Bill of Rights

The U.S. government has codified patients' rights in the Health Insurance Portability and Accountability Act, and the U.S. Department of Transportation provides protections for air travelers. Similarly, the government could extend rights and protections to individual users in cyberspace. Research is needed to define options for a user bill of rights. Cost-benefit analyses for individuals, producers, and government would also clarify the effects of such a policy on the overall cyber ecosystem.[2]

Cyber Education and Awareness

Players believed that there is a role for government either in raising public awareness about cybersecurity and providing a baseline education or in crafting cybersecurity training standards and curricula for public schools at various grade levels. There are many examples of government education campaigns ranging from tobacco smoking to anti-fraud and identity theft awareness that provide precedents and possible models for such efforts.[3] Players who advocated for these solutions implicitly assumed that providing users with better cybersecurity education would lead to improved security across the cyber ecosystem.

[1] The current NIST framework for the cybersecurity of critical infrastructure (NIST, 2014) has generally been well received. However, the Rainbow Series books published in the 1980s and early 1990s by the U.S. Department of Defense and, later, the National Computer Security Center were not as well regarded (see, e.g., Schneier, 1994). Another example is FedRAMP, an ongoing U.S. government effort to provide guidance for the cybersecurity of cloud-based systems (U.S. General Services Administration, undated).

[2] There is much work to be done to design such a document that would encompass both privacy and security issues. Note that a consumer privacy bill of rights has been proposed (White House, 2012), but implementation has not progressed, in part because of concerns about a lack of enforceability (Center for Democracy and Technology, 2015).

[3] One example of this consumer education is the Federal Trade Commission's IdentityTheft.gov portal, which offers information for users who are concerned about their identity being stolen, serves as a reporting mechanism, and outlines an initial response plan for the victim to follow.

Research is needed to understand what effect education actually has on cybersecurity and which forms of cyber education (if any) lead to clear improvements in cybersecurity. Armed with this information, follow-on research could identify the right type and level of government involvement in cyber education, what knowledge and skills should be included, and which audiences should be targeted.

Labeling Standards

At multiple times during game play, participants compared the need for cybersecurity standards to nutrition labels on food products.[4] They described the value in being able to pick up any two food containers and, with minimal effort and no nutrition education, being able to compare which item has more or less fat, sugar, or protein. Players proposed a labeling system for IT products that describes in an easy-to-compare format a product's security, data-sharing and privacy protections, and other relevant information for consumers. The first research task would be to determine whether such labeling would improve cybersecurity enough to justify the potential costs. If there is sufficient return on investment, then further research would help identify the types of products that would be subject to such standards and how to create a useful rating mechanism.

Designing Public-Private Partnerships

Two topics raised during the games could help level the playing field between consumers, who lack transparency into the security of IT capabilities and who individually lack bargaining power with the industry, and IT producers, who need their products to be secure enough to compete in the market but who cannot accept more costs than the market will bear. Bridging this gap will likely require both government and private-sector buy-in, but research is needed to understand the actual impact on cybersecurity and how such partnerships might be implemented.

[4] This could be seen as an expansion of a privacy model suggested by the CyLab Usable Privacy and Security Laboratory at Carnegie Mellon University (Kelley, 2009).

Security Certifications

Certifications are the “stamp of approval” that informs a consumer that a specific product meets a minimum standard. Like Energy Star for consumer products or Leadership in Energy and Environmental Design (LEED) for buildings, a security certification could provide consumers with an easily recognizable security stamp of approval. Some certifications, like LEED, provide tiered levels; under such a system, instead of a single rating, a product could attain silver-, gold-, or platinum-level security. Future research should explore these analogies in depth. In particular, research is needed to determine what effect such certification might have on the cybersecurity ecosystem and whether it would be an effective means of improving cybersecurity.[5] If studies show that such certifications are promising, further research could be directed toward designing the initial framework for a security certification system and recommending whether a government or non-government entity is best positioned to adopt and maintain the system and to certify products.

EULA Standards

EULAs are unfair to users, who cannot choose which terms to accept or reject, and few alternative products are available to users who do not agree to a EULA’s terms, if they bother to read them.[6] EULAs do not merely touch on issues of security; they also deal with privacy, data sharing, warranties, intellectual property, and more. When a EULA does not predict or fully cover every eventuality, it is (more often than not) up to the provider to determine which laws and courts apply.[7] A public-private coalition could develop rules for EULAs specifying the

[5] For existing research on these topics, see, for example, Edelman (2011) and Listokin (2015).

[6] EULAs often contain extremely complicated terms, and users frequently click through without bothering to read them. Even if they chose to spend time reading the agreements, the contracts are often overly long and written in legalese. This can lead users to make assumptions about the terms, only to find out that they have no recourse when a perceived violation has occurred (Ayres and Schwartz, 2014).

[7] Even more problematic is the fact that EULAs govern only the end user–provider relationship, rather than the user-user relationships that often occur. Violating the privacy of

terms that can and cannot be imposed on users and what mechanisms users have to negotiate, opt in or out, or appeal. Research could begin to frame these options, inform the design and roles of a EULA-reform coalition, and examine the potential effects of such standards on the cyber ecosystem, as well as their cost-effectiveness.

Exploring a Diversity of Cyber Ecosystems

Both games described in this report took place in the United States, which inherently influenced the game play: American players shared common values (such as a belief in civil rights and free expression) that are not necessarily prioritized to the same extent in every country. The Washington and Silicon Valley participants also represented various stakeholder groups that already have established positions on many cybersecurity issues. Furthermore, alliances have developed between stakeholder groups, so there is some uncertainty about the independence of the various groups and the ideas they proposed. For these reasons, it would be informative to conduct further cybersecurity-focused 360° Discovery Games in environments that

1. represent cyber ecosystems with potentially different cultures, economic engines, and leadership approaches
2. are expected to offer independent approaches and solutions
3. have less-entrenched positions and fewer established stakeholders.

Having investigated the two centers of mass within the U.S. cyber ecosystem—the Washington Beltway and Silicon Valley—one would expect results from subsequent U.S.-based cybersecurity games to be different in degree but not in kind. For this reason, it would be valuable in the near term to conduct future games in other countries or with multinational groups of participants to explore the effects of cultural,

another user might be seen as a breach of contract with the provider, but the responsible party cannot be held in breach of contract when the victim is another user (Barker 2016).

economic, and leadership biases and to challenge core assumptions of what *security* means in cyberspace. Such games would also serve to both test the fundamental premises of our cybersecurity framework and provide additional insights on both the consistency and relative strengths of the various relationships essential to the framework we presented in Chapter Two.

The European Union, in particular, would provide an ideal venue in that it places a premium on individual rights and freedoms in cyberspace, backed by a strong tradition of privacy and collective solutions. Laws governing data ownership also differ markedly from those in the United States, meeting the first venue criterion. A preference for user- and community-centric solutions would provide insights about the benefits and trade-offs relative to U.S.-focused government or industry approaches. Europe also has a well-developed cyber ecosystem that bridges social values and national economies, satisfying the second venue criterion.

Australia is another interesting venue option. In many ways, Australia is a cybersecurity policy *tabula rasa*: Until recently, it lacked an established and influential cyber policy sector; it did not yet have significant government policies, laws, or established jurisprudence with regard to cybersecurity; it had not yet been a major target for cyber crime organizations; and privacy, civil liberty, and data ownership issues remained in the background. Serendipitously, Australia is the only developed nation whose head of government has a professional background in IT technology and Internet services.[8] Likewise, Australia recently proposed a national cybersecurity strategy.[9] This is simultaneously occurring at a time when Australia and the developed Asia-Pacific economies of Hong Kong, Singapore, South Korea, and Taiwan

[8] Australian Prime Minister Malcolm Turnbull, formerly the country's communications minister, ran a software and investment company and cofounded one of Australia's largest Internet service providers in the 1990s (see BBC News, 2015).

[9] In his foreword to the strategy report, Prime Minister Turnbull said, "This new structure will ensure cybersecurity is given the attention it demands in an age where cyber opportunities and threats must be considered together and must be addressed proactively, not simply as a reaction to future cyber events." See Government of Australia (2016) for the full text of the report.

are becoming increasingly aware of their dependence on IT systems, and their current geopolitical environment has primed them to address cybersecurity challenges. Thus, Australia meets all three of our venue criteria.

Testing and Refining Ideas for a Cybersecurity Framework

In Chapter Two, we presented a preliminary framework for thinking about cybersecurity that was inspired by the two cybersecurity games we conducted. That framework distills stakeholders into four simple "actor" categories (*users*, *developers*, *exploiters*, and *securers*) and simplifies their complex relationships to the essential elements (shown in Figure 2.3 in Chapter Two). In this way, the framework captures at the macro level the behaviors and relationships we observed in the cybersecurity games. The key observation that the relationship of the *securers* with both *users* and *developers* is immature and insufficient aligns with our experience researching cybersecurity challenges. Further, the implied zero-sum relationships between the equities of the *users* (value), *developers* (competitiveness), and *securers* (security) not only fits within our own research experiences, but it also parallels similar zero-sum triangles in other fields, such as acquisition (price, performance, schedule) and thermodynamics (volume, pressure, temperature).

More work is needed to test whether this model is both appropriate and useful. It should be tested in a broad set of environments, with a variety of players, using different scenarios. As we conduct more games, we will explore the implications and inferences outlined in this report, including the nature of the relationships between *securers* and *users* and between *securers* and *developers*, and whether the value-competitiveness-security dynamic truly represents a zero-sum relationship. If this framework holds up to further development and scrutiny, its broad, high-level nature suggests that it might also provide a way to think about other emerging technologies that are driven by market forces and that could have significant consequences if not developed in a secure manner. Genetic engineering is an example of an emerging field that has these characteristics: great potential value for users and great potential for explosive private-sector development, but also significant concerns if the technology is misused or falls into the wrong hands. Perhaps a framework like the one we have proposed for cybersecurity—if it is indeed applicable—could help catalyze thinking on policies in other fields in a way that ensures benefits while also managing risk.

APPENDIX

Organizations Represented in the Games

RAND held two Cybersecurity 360° Discovery Games: one in Washington, D.C., in August 2015 and a second in Berkeley, in California's Silicon Valley, in February 2016. The Chatham House Rule precludes us from identifying the players, but the caliber of the participants is demonstrated by the following list of affiliations. All players were invited on the basis of their expertise as individuals, not as representatives of their organizations, and they were asked to provide their personal perspectives and inputs. The players did not speak on behalf of their organizations, nor did they represent their organizations in any way.

Accenture

Alfred P. Sloan Foundation

American Civil Liberties Union (ACLU)

Bay Area Urban Areas Security Initiative

Blueseed

BMNT Partners

Boing Boing

Brookings Institution

Bugcrowd

California Information Security Office

Carnegie Endowment for International Peace

Center for Democracy and Technology

Center for Strategic and International Studies

Chevron

CISCO

Columbia University, Center for Cybersecurity

Congressional staff

Council on Foreign Relations

Crowd Strike

Daily Beast

Defense Advanced Research Projects Agency (DARPA)

Defense Innovation Unit Experimental (DIUx)

Electronic Frontier Foundation

Electronic Privacy Information Center (EPIC)

Endgame

Federal Bureau of Investigation

FireEye

George Washington University, Center for Cyber and Homeland Security

George Washington University, Cyber Security and Privacy Research Institute

Goldman Sachs

Google

HackerOne

Harvard University, Belfer Center for Science and International Affairs

Harvard University, Berkman Center for Internet and Society

International Computer Science Institute

Inside Cyber

IronNet Cybersecurity

Jones Day

Lawrence Livermore National Laboratory

Massachusetts Institute of Technology, MIT Cybersecurity and Internet Policy Research Initiative

Microsoft

National Security Council

New America Foundation

New York University

Northern California Regional Intelligence Center

Office of the Director of National Intelligence

Office of the Under Secretary of Defense for Policy

Pacific Northwest National Laboratory

Politico

Quantum Planning Group

RSA Security

Salon

Sandia National Laboratory

Signal Sciences

Spectrum

Steptoe & Johnson LLP

Stanford Law School, Center for Internet and Society

Stanford University

Stanford University, Center on Democracy, Development, and the Rule of Law

ThreatSTOP

Trail of Bits

Truman National Security Project

United States Naval Academy

University of California, Berkeley

University of California, Berkeley, Center for Long-Term Cybersecurity

University of California, Berkeley, School of Information

University of California, San Diego

University of Southern California, Information Sciences Institute

U.S. Cyber Command

U.S. Department of Homeland Security

U.S. Department of Justice

U.S. Department of State

U.S. House of Representatives, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

U.S. Navy

Washington Post

Webb Investment Network

White House, Office of Science and Technology Policy

William and Flora Hewlett Foundation

Wired

Yale University

Zurich Insurance Group

References

Ablon, Lillian, "Social Engineering Explained: The Human Element in Cyberattacks," *Cipher Brief*, October 20, 2015. As of July 26, 2016: http://www.rand.org/blog/2015/10/social-engineering-explained-the-human-element-in-cyberattacks.html

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Santa Monica, Calif.: RAND Corporation, RR-610-JNI, 2014. As of July 26, 2016: http://www.rand.org/pubs/research_reports/RR610.html

Australian Government, *Australia's Cyber Security Strategy*, Canberra, 2016. As of July 26, 2016: https://cybersecuritystrategy.dpmc.gov.au

Ayres, Ian, and Alan Schwartz, "The No-Reading Problem in Consumer Contract Law," *Stanford Law Review*, Vol. 66, No. 3, March 2014, pp. 545–610.

Barker, Kim, "Virtual Spaces and Virtual Layers—Governing the Ungovernable?" *Information and Communications Technology Law*, Vol. 25, No. 1, January 2016, pp. 62–70.

Bazzell, Michael, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*, 3rd ed., North Charleston, S.C.: CreateSpace Independent Publishing Platform, 2014.

BBC News, "Profile: Malcolm Turnbull," September 14, 2015. As of July 26, 2016: http://www.bbc.com/news/world-australia-31087843

Beiker, Sven A., and Ryan Calo, "Legal Aspects of Autonomous Driving," Stanford, Calif.: Stanford University, October 2010.

Calo, Ryan, "When a Robot Kills, Is It Murder or Product Liability?" *Slate*, April 26, 2016. As of July 26, 2016:
http://www.slate.com/articles/technology/future_tense/2016/04/a_robotics_law_expert_on_paolo_bacigalupi_s_mika_model.html

Center for Democracy and Technology, "Analysis of the Consumer Privacy Bill of Rights Act," March 2, 2015. As of August 19, 2016:
https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act

Edelman, Benjamin, "Adverse Selection in Online 'Trust' Certifications and Search Results," *Electronic Commerce Research and Applications*, Vol. 10, No. 2, January–February 2011, pp. 17–25.

Federal Trade Commission, IdentityTheft.gov, homepage, undated. As of August 19, 2016:
https://identitytheft.gov

———, "Credit Freeze FAQs," web page, March 2014. As of August 19, 2016:
https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

Goodman, Marc, *Future Crimes*, New York: Doubleday, 2015.

Hartzog, Woodrow, "Privacy and Terms of Use," in Daxton R. Stewart, ed., *Social Media and the Law: A Guidebook for Communication Students and Professionals*, New York: Routledge, 2013, pp. 50–74.

Kelley, Patrick Gage, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder, "A 'Nutrition Label' for Privacy," *Proceedings of the 5th Symposium on Usable Privacy and Security*, New York: Association for Computing Machinery, 2009, Article 4.

Kim, Peter, *The Hacker Playbook 2: Practical Guide to Penetration Testing*, North Charleston, S.C.: CreateSpace Independent Publishing Platform, 2015.

Libicki, Martin C., Lillian Ablon, and Tim Webb, *The Defender's Dilemma: Charting a Course Toward Cybersecurity*, Santa Monica, Calif.: RAND Corporation, RR-1024-JNI, 2015. As of July 26, 2016:
http://www.rand.org/pubs/research_reports/RR1024.html

Libicki, Martin C., David Senty, and Julia Pollack, *Hackers Wanted: An Examination of the Cybersecurity Labor Market*, Santa Monica, Calif.: RAND Corporation, RR-430, 2014. As of July 26, 2016:
http://www.rand.org/pubs/research_reports/RR430.html

Listokin, Siona Robin, "Industry Self-Regulation of Data Privacy and Security," Fairfax, Va.: George Mason University, June 10, 2015.

Luger, E., and T. Rodden, "Terms of Agreement: Rethinking Consent for Pervasive Computing," *Interacting with Computers*, Vol. 25, No. 3, 2013, pp. 229–241.

National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards Publication 200, Gaithersburg, Md., March 2006.

———, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0, Washington, D.C., February 12, 2014. As of August 19, 2016:
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

National Research Council, *Computers at Risk: Safe Computing in the Information Age*, Washington, D.C.: National Academies Press, 1991.

National Science and Technology Council, *Federal Cybersecurity Research And Development Strategic Plan*, Washington, D.C.: Executive Office of the President, February 5, 2016. As of August 19, 2016:
https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf

NIST—*See* National Institute of Standards and Technology.

Richards, Neil, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, New York: Oxford University Press, 2015.

Roesner, Franziska, Tamara Denning, Bryce Clayton Newell, Tadayoshi Kohno, and Ryan Calo, "Augmented Reality: Hard Problems of Law and Policy," *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, New York: Association for Computing Machinery, 2014, pp. 1283–1288.

Schneier, Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Hoboken, N.J.: John Wiley and Sons, 1994.

———, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York: W. W. Norton and Company, 2015.

U.S. General Services Administration, FedRAMP, homepage, undated. As of August 19, 2016:
https://www.fedramp.gov

White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Intellectual Property Privacy and Promoting Innovation in the Global Digital Economy*, Washington, D.C., February 2012. As of July 2016:
https://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Zalewski, Michael, *Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks*, San Francisco: No Starch Press, 2005.

Today's cyber environment presents unlimited opportunities for innovation, interaction, commerce, and creativity, but these benefits also bring serious security challenges. Satisfactory solutions will require building partnerships among public and private organizations, establishing mechanisms and incentives to foster routine information sharing and collective defense, and educating users about their role in thwarting increasingly sophisticated attacks. With a grant from the William and Flora Hewlett Foundation's Cyber Initiative, RAND developed and conducted two cybersecurity-focused discovery games in Washington, D.C., and California's Silicon Valley that aimed to capture the widest possible range of stakeholder perspectives. Participants represented the tech sector, government agencies, think tanks and academic institutions, advocacy organizations promoting civil liberties and privacy, technology users, and more. The goals were to explore opportunities for improving cybersecurity, assess the implications of possible solutions, and develop an initial framework to support debate and inform decisions regarding cybersecurity policies and practices. The games were structured around two plausible cybersecurity scenarios set in the near future. In the first scenario, malicious actors have exploited vulnerabilities in the Internet of Things, causing both virtual and physical harm; in the second, massive data breaches have compromised the financial system, including authentication processes. Participants debated dimensions of each problem in multidisciplinary teams, then shared potential solutions and strategies in a large-group setting. The format and findings of the exercises offer insights that can help guide holistic approaches to addressing future cybersecurity challenges.

RAND NATIONAL SECURITY RESEARCH DIVISION and JUSTICE, INFRASTRUCTURE, AND ENVIRONMENT

www.rand.org

$24.50

ISBN-10 0-8330-9686-9
ISBN-13 978-0-8330-9686-9

52450

9 780833 096869

RR-1700-WFHF