Chapter 18
Cooperation and Free Riding in Cyber Security Information-Sharing Programs

Asmeret Bier Naugle
Sandia National Laboratories, USA

Austin Silva
Sandia National Laboratories, USA

Munaf Aamir
Sandia National Laboratories, USA

ABSTRACT

Even with substantial investment in cyber defense, the risk of harm from cyber attacks is significant for many organizations. Multi-organization information-sharing programs have the potential to improve cyber security at relatively low cost by allowing organizations that face similar threats to share information on vulnerabilities, attacks, and defense strategies. The dynamics of an information-sharing program are likely to depend heavily on interactions between human decision makers. This article describes a system dynamics model of an information-sharing program. The model incorporates decision-making strategies of managers and cyber defenders in each participating organization. The model was used to assess how free-riding behavior is likely to affect the success of a multi-organization information-sharing program. Results shows that free riding may make information sharing more volatile and less beneficial early on, but other factors, including cost savings and the perceived utility of shared information, are likely to create success later in the time horizon.

ORGANIZATIONAL COOPERATION IN CYBER SECURITY

Cyber-attacks pose a major threat to modern organizations. These attacks can have nefarious aims and serious consequences, including disruption of operations, espionage, identity theft, and attacks on critical infrastructure. The ubiquity of interconnected machines and advances in hacking techniques lead organizations to allocate substantial resources to protecting themselves and their customers, clients, and

DOI: 10.4018/978-1-5225-5634-3.ch018

others against cyber-attacks. Even with considerable investment in cyber defense resources, the risk of harm from a cyber-attack is significant for many organizations.

We created a system dynamics model (Azar, 2012; Sterman, 2000) to explore potential dynamics of cyber security information-sharing programs. The effectiveness of cyber defense can likely be enhanced through programs that allow organizations facing similar cyber threats to share information about vulnerabilities, attacks, and defense strategies (ENISA, 2010; MITRE Corporation, 2012). Threats faced by different organizations are often similar, and much cyber defense work may be redundant (Hui et al., 2010). Sharing information might allow organizations to better protect themselves while maintaining or even reducing the resources they dedicate to cyber security (Bier, 2012).

Despite the potential benefits of sharing information, cooperative cyber defense programs are not widespread. Cyber defense teams must balance the potential benefits of cooperation against motivations not to cooperate. For example, if an organization's vulnerabilities are leaked, that organization might become more susceptible to cyber-attacks and face damage to its reputation. Trust in partner organizations is therefore necessary for successful cooperation. Since organizations that are likely to benefit most from cooperating with each other are those that face similar threats, they are also likely to have competitive relationships. Competition for customers, clients, or funding may raise concerns about motive and competitive advantage, making organizations less likely to trust each other. Group inertia must also be overcome, as shifts in both individual habits and organizational strategy are required to establish a successful program.

Increased recognition of the potential benefits of information sharing has led to various proposals and programs for cooperative cyber defense. A United States presidential executive order (The White House, 2013) establishes a framework to create policy to increase security and resilience of the nation's critical infrastructures. A major component of the U.S. strategy is increased communication, including information sharing between public and private sectors (Raduege, 2013). This aspect of cyber security regulation has proven controversial, given the potential for privacy breaches (Economist, 2013). The United States Department of Energy (DOE) recently created the Joint Cybersecurity Coordination Center (JC3), and requires DOE-related entities to report cyber security incidents to the JC3 (US DOE, 2013). Information Sharing and Analysis Center (ISAC) and Information Exchange (IE) models (ENISA, 2010; ISAC Council, 2004; MITRE Corporation, 2012) have been used in various critical infrastructure sectors in the U.S. and Europe, including financial services, electricity, public transportation, and health care sectors, to allow sharing of information about cyber and other threats to critical infrastructure. The ISACs have had varied but limited success, due to hesitancies about distributing sensitive information and delays in data sharing as compared to direct relationships between organizations (MITRE Corporation, 2012). More recently, the U.S. House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA). The legislation would have allowed and encouraged the U.S. government to share information about cyber threats with the private sector, but CISPA was not passed by the U.S. Senate and did not become law. The European Network and Information Security Agency published a document asserting that the key to security is cooperation across citizens, industry, and government (ENISA, 2010), and the European Commission is in the process of designing cyber security legislation with an information sharing component (Economist, 2013).

To better understand potential dynamics and key drivers of information sharing in cyber security, we created a system dynamics model that simulates an information-sharing program involving six generic organizations. The model focuses on the social and organizational dimensions of a potential cooperative relationship, with particular attention paid to decisions about organizational participation. The simulations