Chapter 7.18
Tensions in Collaborative Cyber Security and how They Affect Incident Detection and Response

Glenn Fink
Pacific Northwest National Laboratory, USA

David McKinnon
Pacific Northwest National Laboratory, USA

Samuel Clements
Pacific Northwest National Laboratory, USA

Deborah Frincke
Pacific Northwest National Laboratory, USA

ABSTRACT

Security often requires collaboration, but when multiple stakeholders are involved, it is typical for their priorities to differ or even conflict with one another. In today's increasingly networked world, cyber security collaborations may span organizations and countries. In this chapter, the authors address collaboration tensions, their effects on incident detection and response, and how these tensions may potentially be resolved. The authors present three case studies of collaborative cyber security within the U.S. government and discuss technical, social, and regulatory challenges to collaborative cyber security. They suggest possible solutions and present lessons learned from conflicts. Finally, the authors compare collaborative solutions from other domains and apply them to cyber security collaboration. Although they concentrate their analysis on collaborations whose purpose is to achieve cyber security, the authors believe this work applies readily to security tensions found in collaborations of a general nature as well.

DOI: 10.4018/978-1-60566-414-9.ch003

BACKGROUND

Until recently, especially in government, "need to know" dominated the approach to data sharing and discouraged collaborative efforts. Such a system implicitly presumes that the danger of inadvertent disclosure outweighs the benefits of sharing. Since September 11, 2001, the U.S. government has been painfully learning that "need to know" prevents useful collaboration and makes organizations unnecessarily vulnerable (9-11 Commission, 2004).

But in the modern "need to share" or even "need to collaborate" environment, top-down approaches to incident detection and response are unlikely to be successful. It is necessary to consider other practical approaches that can support protection of shared assets within a collaboration. In this chapter, we discuss exemplar goals of collaboration stakeholders (both within an organization and among multiple cooperating organizations), how conflicts arise among protection goals, how these tensions affect the efficacy of the cooperating parties, and ways that these conflicts may be resolved. We will draw upon examples from the experience of several Department of Energy (DOE) laboratories and their successes and challenges in cooperative cyber security.

The DOE provides a particularly rich environment for discussion of collaboration, because DOE missions often require international scientific collaboration. In contrast to "need to know" environments, DOE scientists must collaborate closely, often sharing unique scientific resources across international boundaries. Even the newer "need to share" approach of transferring information among stakeholders is not sufficient for scientific collaboration: joint development of a shared understanding or new knowledge is not the same as sequential or even parallel knowledge discovery or analysis. Further complicating matters, the DOE contains both some of the most sensitive and most open computing resources in the world.

THE HISTORY AND PROBLEMS OF COLLABORATIVE CYBER SECURITY

On November 2, 1988, a 99-line program changed the world. That program, written by Cornell graduate student Robert Morris, stalled mail servers across the nascent Internet and motivated the first ever multi-organizational, international cooperative computer security effort. The implications of the worm led directly to the founding of the federally funded Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie-Mellon University.

Another pivotal cyber security wake-up call was the distributed denial of service (DDoS) attacks of February 2000. On Monday, February 7, the first of these high profile DDoS attacks was launched against Yahoo. Buy.com, eBay, CNN, and Amazon were also attacked that week. On Wednesday, February 9, the last day of the attacks, the amount of bandwidth consumed by these attacks (some servers received as much as 1 gigabit per second of incoming traffic), combined with curious internet users seeking online information about these attacks resulted in a 26.8 percent performance drop, as compared to the previous week's performance (Garber, 2000). Today, websites are better prepared to handle DDoS attacks partly because of increased cyber security collaborations with their ISPs.

In the past several years, identify theft, phishing, pharming, spyware, and online extortion have become more prevalent, and the economic impacts of cyber crime are more significant than many conventional crimes (Kshetri, 2006). Cyber crimes differ from other crimes because they require technological skills, they have a high degree of globalization, and they are relatively new (Kshetri, 2006). The newness and global reach of these crimes has outpaced traditional law enforcement's ability to detect, deter, and prosecute these crimes. Part of the reason law enforcement seems unable to cope with cyber crime is because there exists very little means for