Information Sharing Challenges in Government Cybersecurity Organizations

Quinn E. Lanzendorfer, Robert Morris University, Moon, USA

ABSTRACT

Cyber-attacks happen faster and more spontaneously than traditional warfare. This cyber landscape offers new challenges to organizations due to its unique nature. Building organizations to defend against cyber terrorism and innovating offensive solutions calls for strong information sharing amongst government and military organizations, as well as industry partners. Using an innovative electronic method to collect quantitative and qualitative data from experts, this study seeks to explore the effectiveness and establishment of information sharing practices and procedures in U.S. government cybersecurity organizations. This study also considers the impact of media leaks and terrorism on information sharing practices and procedures.

KEYWORDS

Cybersecurity, e-Delphi, Information Sharing, Media Leaks, Organizational Change

INTRODUCTION

The nature and flow of information needed for cybersecurity organizations are much different than the demands for the previous four domains of warfare (Lanzendorfer, 2015). Cybersecurity’s presence in the United States Government (USG) structure has been taking shape over the last decade. Preliminary observations reflect reluctances from academia and industry to acknowledge the impact of this phenomenon on cyber teams and the new level of attention to policy and practice. Industry and academia base these assumptions purely on the traditional methodologies. Given the speed of information required for cybersecurity organizations, the style and effectiveness of information-sharing practices are different from those used by past Government organizations. This analysis probes the current state of information sharing practices in USG cybersecurity organizations, the effectiveness of information sharing processes between Government and industry partners, and the impact of media leaks on cybersecurity organizations using the innovative e-Delphi method for collecting data from USG and Industry Research cybersecurity experts.

RESEARCH QUESTIONS

RQ1: Are information sharing practices well-established in USG cybersecurity organizations?

RQ2: Do industry partners that provide products and services to USG cybersecurity organizations have and use effective information sharing processes to communicate needs with the USG and other industry partners?

RQ3: Have media leaks and the fading of lessons-learned from the September 11, 2001 terrorist attacks had a negative impact on information sharing in USG cybersecurity organizations?
LITERATURE REVIEW

Cyberspace is the fifth and most recent domain of warfare (Schreier, 2015). The established domains of warfare that precede cyberspace are land, sea, air, and space (Schreier, 2015). The Defense Science Board (2013) defines cyber as term used to “address the components and systems that provide all digital information, including weapons/ battle management systems, information technology systems, hardware, processors, and software operating systems and applications, both standalone and embedded”.

Cyberspace is “composed of the now two billion computers existing, plus servers, routers, switches, fiber-optic cables, and wireless communications that allow critical infrastructures to work” (Schreier, 2015). Cyberspace is “increasingly used as a theater of conflict as political, economic, and military conflicts are ever more often mirrored by a parallel campaign of hostile actions on the internet [sic]” (Schreier, 2015). Cyberspace lacks an identity when compared to the other domains of warfare. Cyberspace “is not a physical place–it defies measurement in any physical dimension or time space continuum” (Wingfield, 2000). The cyberspace domain of warfare lacks both physicality and identity (Wingfield, 2000). Cyberspace is defined as “a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information– communication technologies” (Kuehl, 2009).

The weapons of warfare were once under the exclusive control of internationally responsible states (D’Souza, 2011). The importance of cyber warfare is that it’s very different than what we’re used to. Cyber-attacks could disable power generators, cut off the military command, control and communication systems, cause trains to derail and airplanes to crash, nuclear reactors to melt down, pipelines to explode, and weapons to malfunction (D’Souza, 2011). Unique coalitions between nations and industry partners will be needed more than ever before and it will be difficult to establish whether cyber-attacks have been conducted by specific state and non-state actors (McNeil, 2010). While acts of war have yet to happen on the Internet, the traditional ways of warfare, policy, and treaties may no longer apply (Kirsch, 2012).

The partnership between the USG and industry will likely be more strained in defending the nation against cyber warfare than traditional warfare examples (Clinton, 2011). Clinton (2011) notes “there is not a simple gold standard or mandatory minimum standard of cyber security, which can cause friction in the relationship between government and private industry”. Clinton (2011) adds that Government and industry are destined for failure because: “There are two fundamental differences in these two evenly yoked partners; government’s fundamental role under the U.S. Constitution is to provide for the common defense; industry’s role, backed by nearly a hundred years of case law, is to maximize shareholder value”.

Effective information sharing improves communication and reduces organizational silos, which in turn improves the expedition and usefulness of intelligence to assist cybersecurity professionals in preventing attacks (Lanzendorfer, 2015). Structuring in Government cybersecurity organizations meets Bolman and Deal’s (2008) six structural assumptions, which are:

- Organizations exist to achieve established goals and objectives;
- Organizations increase efficiency and enhance performance through specialization and appropriate division of labor;
- Suitable forms of coordination and control ensure that diverse efforts of individuals and units mesh;
- Organizations work best when rationality prevails over personal agendas and extraneous pressures;
- Structures must be designed to fit an organization’s current circumstances (including its goals, technology, workforce, and environment);
6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/article/information-sharing-challenges-in-government-cybersecurity-organizations/245281?camid=4v1

This title is available in InfoSci-Journals, InfoSci-Journal Disciplines Computer Science, Security, and Information Technology. Recommend this product to your librarian:

www.igi-global.com/e-resources/library-recommendation/?id=2

Related Content

Development of an Intelligent Patrol Routing System Using GIS and Computer Simulations
www.igi-global.com/chapter/development-intelligent-patrol-routing-system/5271?camid=4v1a

Secure and Efficient Medical Image Transmission by New Tailored Visual Cryptography Scheme with LS Compressions
www.igi-global.com/article/secure-and-efficient-medical-image-transmission-by-new-tailored-visual-cryptography-scheme-with-ls-compressions/127341?camid=4v1a

Keyframe-Based Vehicle Surveillance Video Retrieval
www.igi-global.com/article/keyframe-based-vehicle-surveillance-video-retrieval/210136?camid=4v1a
The State-of-the-Art Technology of Currency Identification: A Comparative Study
www.igi-global.com/article/the-state-of-the-art-technology-of-currency-identification/182465?camid=4v1a