

Building a Digital Commons for Cyber Security Resources

Patricia Erwin

Dartmouth College; Institute for Information Infrastructure Protection, I3P, USA

Abstract

The Institute for Information Infrastructure Protection (I3P) is a consortium that includes academic institutions, federally-funded national laboratories, and non-profit organizations in the United States. The I3P brings experts together to identify and help mitigate threats aimed at the U.S. information infrastructure. Funded by the U.S. Department of Homeland Security (DHS), and the National Institute for Standards and Technology (NIST), the Consortium functions as a virtual national lab, with the ability to organize teams and workgroups to address research and policy-related aspects of the vulnerabilities inherent in the information infrastructure. A core value and long-term goal of the I3P is information sharing. In 2003, this led to the development of the I3P Knowledge Base project. With funding from NIST, the I3P Informatics Services Team was charged with creating a digital commons of cyber security information, tools, and resources for researchers.

Much of the early (2003-2005) information the I3P Knowledge Base provided was temporal, such as the cyber security events calendar and the funding opportunities alert service, or information aimed at the development of the Consortium. As the team began work on the digital library, a host of new challenges were presented. Cyber security, or information infrastructure, is a relatively new area of research, with much of the information about the topic falling into the category of 'grey literature.' While research has been published along the more traditional publication channels, there is valuable research information contained in technical bulletins, presentations, and workshop notes scattered throughout our members' offices and informally organized archives. The information is in a variety of formats, and presents a host of preservation, ownership, and access issues. There also is no fully developed or widely used taxonomy for understanding and categorizing cyber security information. The development of the taxonomy will be a second thrust of the project.

Perhaps the most interesting challenge of this project is how best to balance the need to make available research information in cyber security against certain security and financial risks posed by organizing and making available the information. This presents for the research librarian not only technical and administrative challenges, but also ethical questions.

The goal of my paper is to present a case study, outlining the challenges, the major stakeholders and their roles in creating both challenges and solutions, and the role librarians have played in this project. I believe that the topic of the paper, and the conference focus on open access to grey literature, are an excellent vehicle for this discussion. In examining this case study a number of larger social and political issues will be touched upon. While each of these topics are worthy of more in-depth discussion, I will focus this paper on the building of a cyber security digital commons.

Introduction

Cyber security and information infrastructure protection have emerged as key international issues. The Institute for Information Infrastructure Protection (I3P) was established to promote research to address the potential for cyber threats. The Informatics Services Team has been charged with developing a core set of tools and services aimed at providing access to cyber security information. Central to our mission is creating a digital library, composed of many information types. Much of the information that will be contained in the digital library falls under the definition of grey literature. This paper will outline the proposed development of the Digital Library, the challenges we face in building it, and the very prominent role grey literature contributes to the lasting value of the I3P Digital Library.

The goal of my paper is to present a case study, outlining the challenges, the major stakeholders and their roles in creating both challenges and solutions, and the role librarians have played in this project. I believe that the topic of the paper, and the conference focus on open access to grey literature, are an excellent vehicle for this discussion. In examining this case study a number of larger social and political issues will be touched upon.