I3P Sponsored Project

The Messy World of Grey Literature in Cyber Security

8th Grey Literature Conference
4-5 December 2006
New Orleans, Louisiana

Patricia Erwin – I3P Senior Assistant Director for Informatics Services,
I3P Digital Commons Project Director

Overview of Presentation

- Brief introduction to the Institute for Information Infrastructure Protection (I3P).
- Brief overview of the Digital Commons Project and the Digital Library.
- Four observation on the research activities in general, and specifically how grey literature in cyber security is not addressed in the standard collection development policy.
- An overview of selected I3P Members' library collection development policies.
- How the I3P is addressing the problem.

The Institute for Information Infrastructure Protection (I3P)

- The Institute for Information Infrastructure Protection (I3P) located at and managed by Dartmouth College, Hanover NH.

- Funding for the I3P comes from the US Department of Homeland Security (DHS) Directorate on Science and Technology and the National Institute for Science and Technology (NIST)-soon to also be sponsored by DHS-National Cyber Security Directorate.

- The I3P Consortium is composed of US academic institutions, national labs, and not-for-profit research organizations – all have strong cyber security research programs or focus.

- The I3P Consortium sponsors research projects and programs, including Process Control Systems, the Economics of Cyber Security, and four new projects starting in 2007.

- The Cyber Security Digital Commons is an I3P-sponsored project that includes both public and private information tools and services.

The Digital Commons Project

Mission

We seek to be the electronic conduit through which users learn, collaborate, and create new knowledge in the broad area of information infrastructure protection. Our unique approach will be the emphasis on scope, making it the first place the cyber security community [and others] turn to for what is happening in the world of information infrastructure protection.

Tools and Services

- International Calendar of Cyber Security Events
- International Cyber Security Organization Directory
- Cyber Security Glossary
- Cyber Security Digital Library

The Details

- **How We Provide Value**
  - **Quality** – Information is selected based on established criteria
  - **Focused** –Targeted body of knowledge
  - **Fast –** What we cover is in one location
  - **Unique –** Resources you can't find other places
  - **Free –** Anyone can use our services

- **Targeted Customer Base**
  - **Researchers** (academia, industry, and government)
  - **Librarians & Information Professionals** (information providers to researchers)
  -
  - **Industry Users** (interested in standards & solutions)
  - **Public** (interested in answers they can understand)

Recent Changes

I3P Review

- As an I3P-sponsored project, we were reviewed in September 2006.
- Focus was primary feedback.
- Value of grey literature.

Going Forward

- Workshop outcomes
- Lesson plans and training materials
- Research team discussions
- Internal technical reports
- Random charts, planning sheets, thought papers, etc.

This was a recognition that no other organization was doing this in a systematic manner, making the information publicly accessible, or planning for its' long-term preservation.

Grey Literature Produced by the Consortium

Characteristics

- Not previously published through the standard or commercial publication channels.
- In a variety of formats and conditions.
- May have use restrictions.
- Authorship and/or ownership may be unclear.
- Research value may be unclear – hard to predict for the future.

Four Observations

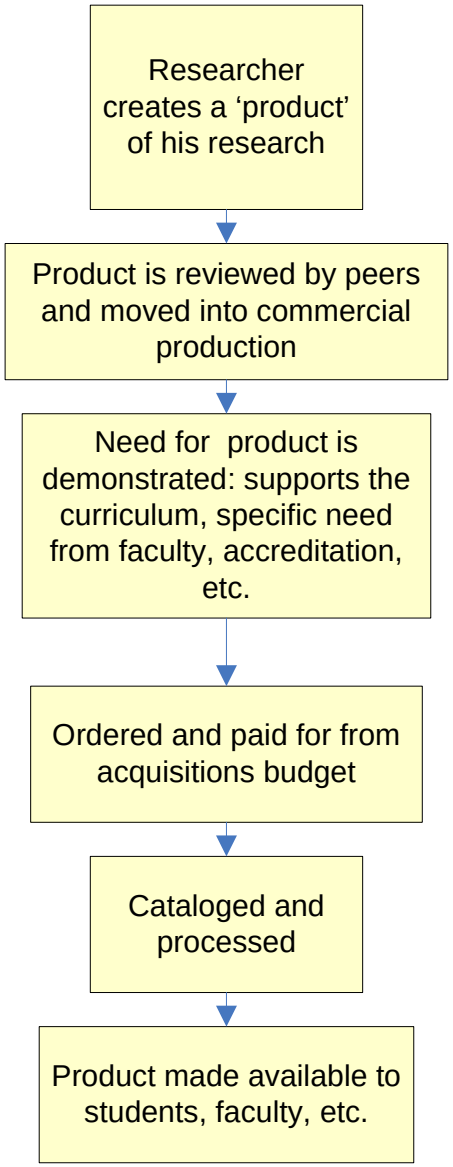
Research is messy - We are attempting to formally capture information that normally flows through an informal process.

Traditional collection development policies are structured documents aimed at assuring a level of quality in the collection, but also to satisfy the administrative needs to justify the expense of providing resources to an academic or research community

Grey literature doesn't fit the formal model of scholarly communication, therefore the quality is suspect and is not adequately addressed in most collection development policies.

The research process and grey literature share similar attributes.

Traditional Collection Building Process



- Linear
- Organized
- Information treated like a product
- Auditable
- Justifiable
- Predicable
- 'Easy'

We Like this process!

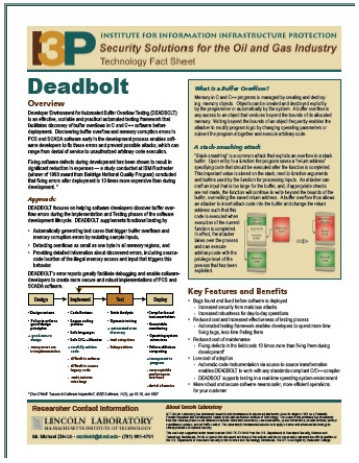
Grey Literature Mirrors the Research Process

I3P Grey Literature Tangibles

Samples of What Non-Traditional Items We Harvest

Story Maps

Project Fact Sheets



Irregularly Published Bulletins

These Resources Might Not be Collected Under a Traditional Collection Development Policy

I3P Consortium Members – Grey Literature Collections

- **National Laboratories:** Collect their own in-house technical reports and training materials. These are generally not publicly accessible and do not appear in their catalog display open to the public.

- **Academic Libraries:** This resources would not be routinely collected, cataloged or preserved. May be stored in department files, sponsored research ‘closed’ project files, or in exceptional cases, the college archives.

- **Not-for-Profit Research Organizations:** Collect their own in-house technical reports and training materials. These are generally not publicly accessible. Library catalogs are not usually open to the public.

Researchers find out about these resources through an informal research network. The Digital Commons Project is attempting to make this process part of a formal collection ‘access’ policy.

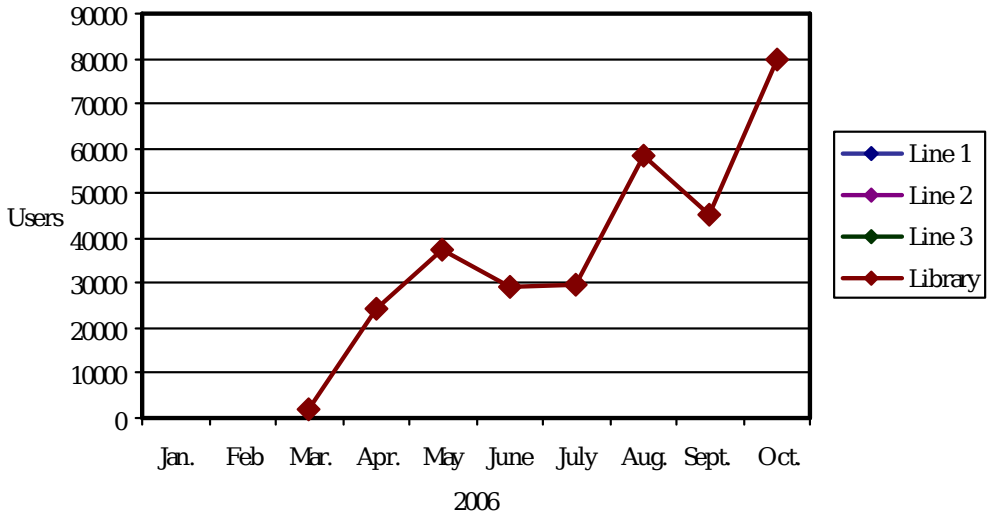
Special Projects & Focus

- UC Davis Project- digitizing, preserving, and cataloging resources from the Computer Security History Project.

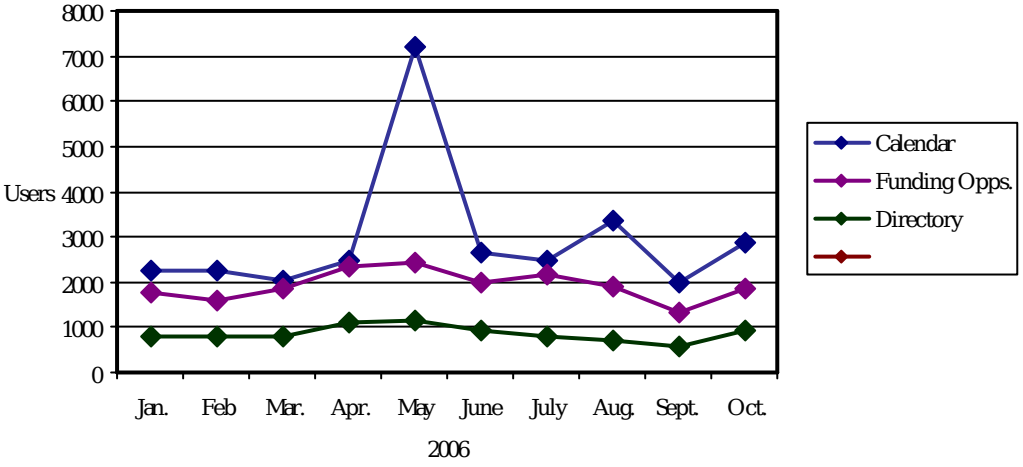
- Cyber Security Training Materials: This would be a great service to practitioners, students, and researchers, but many obstacles.

Are We Being Used?

Digital Library



Other Digital Commons Services



Conclusion

New Model for Collection Development Needed for Cyber Security

- **Focus on the ‘fruits’ of research.**
- **Unique materials.**
- **Not always easy to capture-new approaches are needed.**
- **Mirror social aspects of research.**
- **Acknowledge the value is subjective- future may determine value.**

To Learn More about the I3P Digital Commons of Cyber Security Information

http://digitalcom.thei3p.org/