

CUCCIO Information Security SIG Status Report – CANHEIT 2008

Membership Summary as of June 1, 2008:

# of Institutions	29
# of Participating Members	34

A list of member institutions is available on the CUCCIO web site.

Meetings Summary:

Mtg #	Date	# of Member Institutions	# Present	% Present	Major Topic(s)
1	24-Apr-07	22	15	68%	Planning for initial meeting at CANHEIT 2007
2	29-May-07	25	18	72%	Terms of reference review, initial discussions
3	16-Aug-07	25	15	60%	Collaboration tools, priorities survey, CANHEIT 2008 discussion
4	19-Oct-07	27	12	44%	Priorities discussion & CANHEIT 2008 responses review
5	1-Jan-08	28	14	50%	Focus group updates & CANHEIT 2008 discussions
6	5-Feb-08	30	13	43%	Updates on priorities, CANHEIT program development
7	6-Mar-08	30	9	30%	Updates on priorities, CANHEIT program, incident communications
8	1-Apr-08	29	16	55%	Priorities, CH08 program finalized, IR communications, media disposal
9	29-Apr-08	29	10	34%	Priorities & CH08 updates, incident response & comms, spearphishing attempts
10	27-May-08	29	8	28%	CH08 InfoSec Panel planning, secure coding, PCI compliance
11	16-Jun-08	29			Meeting at CANHEIT 2008 (Calgary) - education focus

2007/2008 SIG Activity:

1. Continued focus on three topics, prioritized based on a survey of the SIG membership:
 - Policies & Procedures (including “Local Access Management” as an initial focus)
 - Multi-factor Authentication
 - Incident Response

2. CANHEIT 2008 program support:
 - The SIG had the leading role in defining the “Security & Infrastructure” stream for CANHEIT 2008.
 - SIG co-chairs from Queen’s University and the University of Western Ontario were joined on the CANHEIT 2008 Program Committee by the SIG member from the University of British Columbia.

- SIG members contributed the overwhelming majority of submissions to this program stream.
 - Sufficient numbers of submissions were received to warrant a “Security *only*” stream, with the smaller number of “Infrastructure” submissions merged with “Support” submissions into a “Support and Infrastructure Models” stream.
 - SIG members are responsible for all but one of the Security sessions selected for the final program.

3. Communication:

- Email/list-based communication is ongoing among SIG members on a wide variety of topics.
 - On average, approximately 3 topics are raised and discussed each month through the email lists.
- The number of SIG member institutions participating in [REN-ISAC](#) continues to grow, the premier source for “information collection, analysis and dissemination, early warning, and response,” related to information security within higher education.
 - This approach echoes the terms of reference and the SIG’s efforts to provide value to members based on the uniqueness of the Canadian Higher Education IT environment. (see [Appendix B](#)) or the CUCCIO web site at:
 - Attempting to replicate [REN-ISAC](#)’s mandate would neither provide unique benefits to the membership, nor would it be an efficient use of member resources.
- A relationship has been struck for the communication of advance, intelligence-based warnings from the Canadian government’s [CCIRC](#) body to SIG members.
 - This communication channel allows for alerts to the SIG membership as a whole, as well as for targeted alerts in the presence of specific intelligence relating to one or more member institutions.
 - In future, this relationship may spur additional interaction between provincial incident response agencies and SIG member institutions.
- Monthly meetings of the SIG members, and regular meetings of members working on the priority topics noted above, will continue through 2008 and onward.

The Terms of Reference for the SIG were approved in April 2008 and can be found on the CUCCIO web site at:

http://www.cuccio-cdpiuc.ca/files/SIG-terms/CUCCIO_Security_SIG_Terms_of_Reference.pdf

Appendix - Glossary & External Links

CCIRC	<p>Canadian Cyber Incident Response Centre</p> <p>http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx</p> <p>“The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring threats and coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents.”</p>
REN-ISAC	<p>Research & Education Networking – Information Sharing & Analysis Centre</p> <p>http://www.ren-isac.net/</p> <p>“Supported by Indiana University and through relationship with EDUCAUSE and Internet2, the REN-ISAC is an integral part of higher education’s strategy to improve network security through information collection, analysis and dissemination, early warning, and response -- specifically designed to support the unique environment and needs of organizations connected to served higher education and research networks; and supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC structure.”</p>