The Report of the

2016 Cybersecurity Summit for

Large Facilities and Cyberinfrastructure

Strengthening Trustworthy Science

August 16 - August 18

Westin Arlington Gateway - Arlington, VA

http://trustedci.org/2016summit

Acknowledgements

The organizers wish to thank all those who attended the summit. Special gratitude goes to all those who responded to the CFP, spoke, provided training, and actively participated, including the 2016 Program Committee (highlighted in Section 3), without whom the event would not have been as successful. Our sincere thanks goes to the National Science Foundation and Indiana University's Center for Applied Cybersecurity Research for making this community event possible.

This event was supported in part by the National Science Foundation under Grant Number 1547272. Any opinions, findings, and conclusions or recommendations expressed at the event or in this report are those of the authors and do not necessarily reflect the views of the National Science Foundation.

About this Report

Drafts of this report were circulated for comment to the Program Committee (1/6/2017) and summit participants (1/13/2017).

Citing this Report

Please cite as: James Marsteller, Von Welch, Amy Starzynski Coddens. Report of the 2016 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities: *Strengthening Trustworthy Science*. http://hdl.handle.net/2022/21161

For the latest information on the Summit

Please see, https://trustedci.org/summit/

Table of Contents

Executive Summary

The 2016 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure continued to build a trusting, collaborative community working to address core cybersecurity challenges in support of NSF science. The 2016 summit built on the success, findings, and lessons learned from previous years, and focused on the theme of Strengthening Trustworthy Science. The program committee and presentations submitted by community members drove the program. A call for participation(CFP) resulted in nineteen (19) proposals including a mix of 9 case study and general presentations, 2 panel topics, and 8 training sessions. For the second year in the row, the summit received a marked increase in CFP proposals, again exceeding our capacity to accommodate.

The 2016 summit took place in Arlington, VA, August 16th through midday August 18th. On August 16th, it offered a full day of training. The second and third days followed were plenary sessions designed to address the theme of Strengthening Trustworthy Science in the context of cyberinfrastructure projects and Large Facilities.

One hundred individuals attended the summit, with 45 individuals -- almost one half of all registrants -- participating in planning, speaking, providing training, co-authoring a CFP submission, and/or leading a lunch table talk. In all, 44 NSF-funded projects, including 14 Large Facilities, were represented. Attendee evaluations and feedback were overwhelmingly positive and constructive.

The Summit continued to make progress on recommendations and opportunities defined at the 2016 Summit. A full list of recommendations and opportunities is in Section 7 of this report, but the following are the Priority Recommendations and the progress made at the 2016 Summit:

Recommendation 1: The NSF CI and Large Facility community should develop a broadly applicable strategy for information security budgets, including how, why, and where it does what it does in terms of spending.

Progress towards Recommendation 1: A number of presentations mentioned budgetary issues and the following data points were presented:

- A case study of DOE Science Labs security budgeting showed average security budgets lie between 3% to 12% of the IT budget;
- a Forrester study showing security spending between 1-13% of IT budgets with 5.6% being the average; and
- the U.S. Antarctic Program information security budget is equal to 12.5% of the total IT budget.

Recommendation 2: The NSF CI and Large Facility community should support research on metrics that indicate whether spending on information security is sufficient and appropriately balanced with a project's science mission.

Progress towards Recommendation 2: Presentations from LIGO, GENI, and the NSF Polar Program discussed metrics subjectively, e.g. *"LIGO [security] policy is to properly plan and implement security in a way that supports the scientific mission in a minimally intrusive manner that enables reliable access to data and use of LIGO."*

Recommendation 3: The NSF CI and Large Facility community should develop a common understanding among all stakeholders of how accountability, risk responsibility, and risk acceptance practices are most efficiently and appropriately distributed among project leadership, project personnel, and other stakeholders.

Progress towards Recommendation 3: Presentations from NCAR and LIGO discussed the importance of having management assume responsibility for risk acceptance. A presentation from GENI described that projects framework for defining and sharing responsibility.

Recommendation 4: The NSF CI and Large Facility community should determine its software assurance, quality, and supply chain requirements.

Progress towards Recommendation 4: A presentation from LIGO described software reviews as part of its cybersecurity program.

1 Background: Evolving Cybersecurity Landscape, and Advancing Trustworthy Science

Cybersecurity is a fast-developing and challenging field for all organizations in our contemporary world. The challenge is amplified by the intersection of myriad factors, including rapidly changing technology; ever-evolving and diverse threats; lagging workforce development; economic challenges; asymmetries in the cost and difficulty of attack and defense; and the nascent state of cybersecurity practice in general.

NSF awardees face distinct questions when initiating information security programs due to their projects' unusual, and often unique, combination of attributes: distributed, collaborative organizational structures and relationships with other entities (*e.g.*, campus); unique, costly scientific instruments; limited resources, talent availability, and timelines; diversity in communities and missions; open, yet irreplaceable scientific data with an unclear threat model; and the need for reproducibility and maintaining public trust in their resulting science.

A number of well-known frameworks for cybersecurity exist, but they continue to evolve and none have emerged as a clear best practice. For example, NIST's *Framework for Improving Critical Infrastructure Cybersecurity*[1] and the National Strategy for Trusted Identities in Cyberspace (NSTIC)[2] propose important approaches for cybersecurity programs and identity management. However, best practices for the federal government, commercial companies, and even research labs and institutions of higher education, do not directly translate to scientific communities and computing infrastructure.

In addition to the cybersecurity efforts and experiences of individual NSF projects, and the research advances of the NSF Secure and Trustworthy Cyberspace (SaTC) community, NSF has funded cybersecurity resources for the NSF community in the form of the extension of CTSC as the NSF Cybersecurity Center of Excellence (CCoE)[3] and the Bro Center of Expertise[4]. Additionally, NSF has funding for applied cybersecurity for science available under the Cybersecurity Innovation for Cyberinfrastructure (CICI)[5] program. These resources provide focal points for aggregating experiences, and translating the work from the broader world into cybersecurity practices effective for NSF scientific computing.

CTSC, now in its fifth year, reestablished the NSF cybersecurity summits means to reinvigorate

[1] http://www.nist.gov/cyberframework/
[2] http://www.nist.gov/nstic/
[3] http://trustedci.org/
[4] https://www.bro.org/nsf/
[5] http://www.nsf.gov/pubs/2015/nsf15549/nsf15549.htm

the NSF cybersecurity community and increasing out trust of the science supported by that community. Spanning six years from 2004 to 2009 and then reinstated in 2013, the annual NSF Cybersecurity Summits serve as a valuable part of the process of securing NSF scientific cyberinfrastructure (CI) and increasing our trust in the science it supports by providing a forum for education, sharing experiences, and building community. For many attendees, the summits are unique opportunities to come together with their colleagues, to benchmark and debate cybersecurity best practices, and to receive practical, relevant training.

The 2016 summit took place Tuesday, August 16th through midday Thursday, August 18th, at the Westin Arlington Gateway near NSF. On August 16th, the summit offered a full day of training in response the strong training attendance in both 2014 and 2015 and overwhelmingly positive feedback. The second and third days followed a workshop format designed to identify both the key cybersecurity challenges facing Large Facilities and the most effective responses to those challenges. The event brought together leaders in NSF CI and cybersecurity to continue the processes initiated in 2013: building a trusting, collaborative community, and seriously addressing that community's core cybersecurity challenges.

The remainder of this report outlines the summit's organizational process, the resultant program, details on attendance and participation, and results of attendees' evaluations of the event. The report concludes with Recommendations and closing thoughts of the organizers.

2 The Summit's Purpose, Scope, and Theme

The 2016 summit built on the Recommendations of the 2015 summit[6], which was well received both as an educational opportunity and a community networking event. We organizers believe the summits can go even further, and support measurable progress on the following goals: identifying, establishing and sharing community standards for best practices regarding cybersecurity; providing pragmatic levels of information security; meaningfully addressing software assurance, quality or supply chains in the context of the project cybersecurity programs; and supporting scientific discovery.

The recommendations of the 2015 summit served as drivers for the 2016 event:

> *2015 Recommendation 1*. The NSF CI and Large Facility community should develop a broadly applicable strategy for information security budgets, including how, why, and where it does what it does in terms of spending.
>
> *2015 Recommendation 2*. The NSF CI and Large Facility community should

[6] See the 2015 summit report, agenda, and more at http://trustedci.org/2015summit/

support research on metrics that indicate whether spending on information security is sufficient and appropriately balanced with a project's science mission.

2015 Recommendation 3. The NSF CI and Large Facility community should develop a common understanding among all stakeholders of how accountability, risk responsibility, and risk acceptance practices are most efficiently and appropriately distributed among project leadership, project personnel, and other stakeholders.

2015 Recommendation 4. The NSF CI and Large Facility community should determine its software assurance, quality, and supply chain requirements.

The 2015 event focused on Information assets that enable science which entail the production, maintenance, and use of valuable (and sometimes one-of-a-kind) information systems and data.

For 2016, we determined to focus efforts around the theme, ***Strengthening Trustworthy Science,*** to highlight the 2015 recommendations on software assurance, risk responsibility/acceptance, security budgeting and program metrics.

3 The Organizing and Program Committees

The 2016 summit was organized and hosted by the NSF Cybersecurity Center of Excellence, and six members of that project (Ryan Kiser, Jim Marsteller, Susan Sons, Jim Basney, Amy Starzynski Coddens, Von Welch) along with Leslee Cooper, the Administrative Director for the IU Center for Applied Cybersecurity Research, served as the organizing committee. We recruited a Program Committee (PC) made up of key leaders from NSF CI projects and the broader community. The PC was to be responsible for setting the agenda and inviting speakers, evaluating and selecting from among proposed training, talks and panels, extending invitations to expert presenters, participating actively in the event itself, and laying the framework for successful post-summit evaluation and community support. Jim Marsteller served as chair of the PC, a role he has held in prior summits. The PC held 17 meetings by conference call beginning February 23, 2016 and ending August 23, 2016. It conferred electronically both prior to and following this time period, with monthly meetings.

The 2016 PC members were:

- **Steve Barnet,** Senior System Administrator for the IceCube Neutrino Observatory.
- **Anthony (Tony) Baylis**, Assistant Department Manager for the Computing Applications and Research Department in the Computation Directorate at Lawrence Livermore

National Laboratory.

- **Michael Corn**, Deputy CIO and CISO for Brandeis University.
- **Barbara Fossum**, NEES deputy center director and former managing director of Purdue University's Cyber Center and Computer Research Institute.
- **Ardoth Hassler**, Associate Vice President of University Information Services & Executive Director, Office of Assessment and Decision Support at Georgetown University and former Senior Information Technology Advisor in the Office of the Chief Information Officer in the NSF Office of Information and Resource Management, Division of Information Systems.
- **Susan Ramsey**, Risk Assessor and Security Engineer at the National Center for Atmospheric Research.
- **George Strawn**, NAS as board director for the Board on Research Data and Information, Formerly NSFnet program director and then division director of networking), then CISE executive officer and acting assistant director, and then served as CIO. He was detailed to OSTP in 2009 where he served as director of the NITRD NCO .

4 The Call for Participation and Program

The full agenda and biographies are attached to this report as Appendices A and B[7].

The PC issued a call for participation (CFP) to the community requesting submissions in the form of: (a) white papers one to five pages in length, focused on unmet cybersecurity challenges, lessons learned, and/or significant successes, (b) one to two-page abstracts for proposed half and full-day trainings, (c) one to two page abstracts for proposed table talk sessions, or (d) student applications.[8] Additionally, the PC invited specific community leaders as well as experts from outside the community to give presentations and participate in panels.

The CFP continued a process started in 2014, designed to elicit a greater degree of community participation in developing the agenda, executing the summit, and increasing our ability to identify summit findings that represent the concerns, successes, and aspirations of our community. The 2014 CFP process was expanded in 2015 and 2016, and a "Tips for Building CFP Responses" was provided to guide and encourage respondents and additional content formats

[7] The full summit program is also available on the CTSC website, http://trustedci.org/s/ProgramAgenda-2016Summit-SourceDocument.pdf

[8] http://trustedci.org/2016-nsf-cfp/; see also Appendix C.

were considered. All submitted white papers are collected in Appendix D. The CFP process proved a success, and drove a great deal of the resultant program, including a mix of 9 case study and general presentations, 2 panel topics, and 8 training sessions, as well as a keynote from the cybersecurity community at large, and presentations from key leaders from within the NSF community. For the second year in the row, we received a marked increase in CPF proposals, again exceeding our capacity to accommodate.

The Summit program spanned two and a half days from August 16 through 18. On August 16th, we offered a full day of training. Descriptions of each training session are appended as Appendix E.[9] On August 17th and 18th, the Summit followed a plenary format with talks invited by the program committee and accepted from the CFP responses. Dr. Irene Qualters, Division Director of NSF/ACI welcomed the attendees and Peter Kuper of In-Q-Tel gave an invited keynote. The program of submitted talks then commenced with talks on the NSF Cybersecurity Center of Excellence, and lessons learned at Gemini, LIGO, and TACC. Talks then followed on the topics of Science DMZ as a Security Architecture, Cybersecurity Budgeting, and Provenance Based Security. The first day then concluded with talks on the topic of identity management from FermiLab and the Globus Project, and an open discussion session.

Day two opened with a retrospective on FBI Major Case 216 (aka the "Stakkato Incident") that spurred the original launch of the Summit in 2004. Presentations then continued with a overview of GENI cybersecurity, and presentations on adapting the NIST Risk Management Framework to the NSF Cooperative Agreement for Large Facilities, and a panel on compliance (FISMA, FERPA, and HIPAA). Another open discussion session concluded the summit.

5 Participants

For the first time in the summit's history, we opened registration to all interested individuals. This was done to avoid being insular, maintain and develop new relationships, and encourage infusion of additional perspectives. Registration was granted to all parties who requested attend and were able to demonstrate a connection to the community. As with prior summits, registration was free, and, as in previous years, invitations were sent to a predetermined list of individuals. Our invitation list was based on the invitation list from the 2015 summit, and was updated to account for changes in the community, suggestions from NSF staff, and speakers to address specific topics of the summit. The invitation list included those with direct cybersecurity responsibilities in NSF Large Facilities and CI projects, NSF project principal investigators, and other key stakeholders and risk owners to ensure that NSF cybersecurity

[9] See also, http://trustedci.org/2015training/

evolves to address their needs.

Fig 1. Attendees from the 2016 NSF Cybersecurity Summit.

One hundred forty two (142) individuals requested registration for the summit, 121 registered, and 100 attended (including speakers, tutorial presenters, panelists, students and the program committee). A listing of the attendees and their affiliations is in Appendix G. Seventy one attendees participated in the August 16 training sessions. Forty five individuals - almost one half of participants - participated in planning, spoke, provided training, co-authored a CFP submission, and/or led a lunch table talk. Five attendees were students. Twenty four attendees work at Large Facilities. Twelve attendees work at the NSF.

5.1 NSF Project Representation

Attendees were asked to provide the NSF project or other organization (NSF directorate in the case of NSF staff) with which they were associated. The following list contains the provided answers. We count 44 projects including 14 Large Facilities (marked with "♦"), were represented at the summit by representatives of those projects. Additionally, eight more Large Facilities were represented by NSF program officers (marked with "♦*"). NSF directorates represented by program officers only are marked with "*". NSF directorates represented in some manner include: CISE/ACI, CISE/CNS, ENG/CMMI, GEO/AGS, GEO/EAR, GEO/OCE, GEO/PLR, GEO/PLR, MPS/AST, MPS/DMR, and MPS/PHY. Additionally NIH/NIGMS and DOE/ESnet were represented.

We note some answers given represent NSF projects (e.g. "CC*IIE") or other general areas of the NSF community (e.g. "Science Gateways") which are not very precise and we will work on obtaining more precise specification of awards in future summits to improve our understanding of community representation.

- Atacama Large Millimeter Array (ALMA) ♦
- Advanced Modular Incoherent Scatter Radar (AMISR)
- Arecibo Observatory (AO) ♦*
- A Toroidal LHC Apparatus (ATLAS) ♦* Detector
- Association of Universities for Research in Astronomy, Inc. (AURA)

- Building Community and Capacity in Data Intensive Research in Education (BCC)
- Blue Waters
- Bro Center of Expertise
- CC*DNI/CC-NIE
- CC*IIE
- Center for Trustworthy Scientific Cyberinfrastructure (CTSC)
- CILogon
- Cornell High Energy Synchrotron Source (CHESS) ♦
- Compact Muon Solenoid Detector (CMS)♦*
- Cybercorps: Scholarship for Service
- Cyber-Enabled Discovery and Innovation (CDI)
- Cyber-Enabled Materials, Manufacturing, and Smart Systems (CEMMSS)
- Cyber-Physical Systems
- Cybersecurity Innovation for Cyberinfrastructure
- Data Infrastructure Building Blocks (DIBBs)
- Dark Energy Camera (DECam)
- Daniel K. Inouye Solar Telescope (DKIST) ♦
- EarthCube (EAGER)
- Extreme Science and Engineering Discovery Environment (XSEDE)
- Faculty Early Career Development (CAREER)
- Geodesy Advancing Geosciences and Earthscope (GAGE) ♦*
- Green Bank Telescope (GBT)
- Gemini Observatory ♦
- GENI Engineering Conference
- Historically Black Colleges and Universities Undergraduate Program (HBCU-UP)
- HTCondor
- IceCube South Pole Neutrino Observatory (IceCube) ♦
- International Ocean Discovery Program (IODP) ♦
- Laser Interferometer Gravitational-Wave Observatory (LIGO) ♦
- Large Synoptic Survey Telescope (LSST) ♦
- Major Research Instrumentation Program (MRI)
- National Center for Atmospheric Research (NCAR) ♦
- National Center for Supercomputing Applications (NCSA)
- National High Magnetic Field Laboratory (NHMFL) ♦
- National Optical Astronomy Observatory (NOAO) ♦
- National Radio Astronomy Observatory (NRAO) ♦
- National Solar Observatory (NSO) ♦
- Natural Hazards Engineering Research Infrastructure (NHERI) ♦

- Ocean Observatories Initiative (OOI) ♦*
- Open Science Cyberthreat Profile Working Group
- Open Science Grid (OSG)
- Pittsburgh Supercomputing Center (PSC)
- Rapid Response Research (RAPID)
- Summer of Applied Geophysical Experience (SAGE) ♦*
- Science Gateways
- SciDaaS
- Secure and Trustworthy Cyberspace
- Small Business Technology Transfer Program (STTR)
- Stampede (TACC)
- SURE: Summer Undergraduate Research in Engineering/Science
- Sustain-GT
- US Antarctic Program ♦*
- University-National Oceanographic Laboratory System (UNOLS)*
- Very Large Array (VLA) ♦
- Very Long Baseline Array (VLBA)

Participation from NSF program officers at the Cybersecurity Summit was lower this year than in previous years, with 12 attendees as opposed to the 18 that attended in 2015. We note next year NSF will be in process of moving from Arlington to Alexandria, which could also impact attendance in 2017. We are considering these facts at this time and have no definite plan to react.

5.2 Student Representation

In addition to professionals, the Summit supported the participation of five students. Students were encouraged to self-nominate to the program, but were also able to be nominated by a mentor or teacher. In order to be further considered, they were then asked to provide a one-page, 800-word maximum letter describing the student's interest in and any relevant experience with cybersecurity, emphasizing the benefit to the student and/or community of the student's attendance at the Cybersecurity Summit.

The Program Committee reviewed all 10 submissions with an interest in advancing diversity and inclusiveness, settling on the following exceptional five students: Deja T. Jackson (Kennesaw State University), Dominique Dalanni (California State University, Dominguez Hills), Nikita Golubets (Eastern Michigan University), Rasib Khan (University of Alabama at Birmingham), and Vitaly Ford (Tennessee Tech University).

The selected student applicants were paired with mentors from the program committee and community to encourage their continued participation in cybersecurity and NSF cyberinfrastructure. Students and mentors were given one another's contact information prior to the summit and encouraged, but not required, to contact one another. However, each pair did communicate prior to the summit, allowing them to familiarize themselves with one another prior to meeting in person. Once at the summit, students and mentors met each day for breakfast and lunch, along with one night for the program committee dinner. These meet-ups allowed the students to ask any questions they may have and assist in networking, while allowing mentors to introduce and share the community with potential new members.

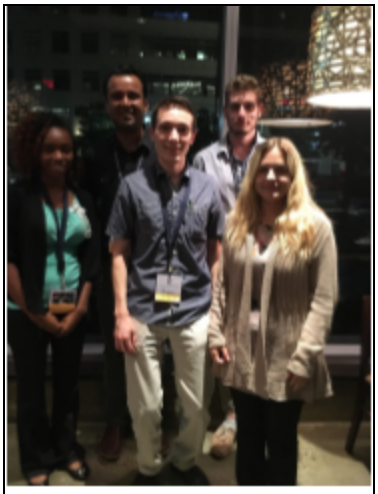


Fig 2. Students from 2016 NSF Cybersecurity Summit

This program has shown success, and we have received positive feedback from both students and mentors. One student in particular stated after this summit:

"I had such an amazing time at the conference and I just wanted to thank you all for being so welcoming. I learned so much and gained exposure to so many different topics that I didn't even know existed. I truly had a wonderful experience so thank you and it was lovely meeting you all." (Dominique Dalanni, California State University, Dominguez Hills).

5.3 Inclusiveness

Finding 4 from the 2013 summit stated "Future program committees should take on gender, age, and racial/ethnic diversity in the community and summit attendance as a strategic imperative for future summits." The organizers recognize that diverse participation is both a socially relevant outcome for NSF[10] and a particular challenge in the cybersecurity community in general[11]. Thus, in 2014, we expressly addressed the topic with the PC, identifying two members to spearhead efforts (Baylis, Hassler), and the group sought to encourage diverse participation via the invitees, speakers, panelists, and PC itself. Additionally, the CFP expressly gave priority to those students from groups underrepresented in the NSF information security workforce. We note that Baylis has specific experience in this area as chair of the

[10] *See*, NSF GPG, Section II.C.2.d.i

[11] *See, e.g.*, *Agents of Change: Women in the Information Security Profession.* A whitepaper derived from the 2013 (ISC)2 Global Information Security Workforce Study. Available from: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf

Supercomputing Broader Engagement in 2008 and participated in that committee in 2009. Baylis and Hassler again spearheaded these efforts in 2016, building on the success seen in 2014 and 2015.

In order to gather ongoing baseline data related to this diversity effort, 2016 registrants had the option to provide their ethnicity/race and gender/sex. There was a small decrease in the number of female registrants in 2016, and a slight change in the ethnicity/race of registrants, with an increase in diverse participants. The aggregated responses to the those items follow. Voluntary responses to these questions show:

Table 1. Attendee self-reported ethnicity.

Ethnicity / Race	
Asian or Southeast Asian	8
Black or African American	3
Hispanic or Latino	3
Native Alaskan or American Indian	0
Multiracial	0
White or Caucasian	60
Other Ethnicity	0
Other (space provided)	0
Prefer not to answer	5
No Answer Provided	21

Table 2. Attendee self-reported gender.

Gender / Sex	
Female	16
Male	59
No Answer Provided	25

6 Attendee Evaluations

We sought attendee evaluations of the summit via two SurveyMonkey surveys. One survey gathered feedback on the summit generally; the other requested feedback specific to the August 16 training sessions.

6.1 Attendee Survey

A summary of the general survey results is appended to this report as Appendix H. The responses were generally very positive and extremely thoughtful, with responses to Question #13, "How can we improve the summit experience in the future?," seeing attendees requesting slight logistical changes and requesting that CTSC continue what they are doing with some adjustments. One attendee captured this theme with the response *"Identify a common theme (or multiple common themes) that can be addressed and presented throughout the summit. This year, for example, there were multiple references to keeping upper management involved in cybersecurity. There were several interesting ideas on how to best approach this, others addressing the reasons to do this, however, it seemed as though this was simply a conclusion that each center has come to during the life of their cybersecurity projects. Maybe a community poll to identify issues that each center is struggling with will identify these common themes that can be discussed and shared at the summit."* Another attendee stated *"Is it feasible to tack on some extra time, for example having it end in the afternoon rather than at 12/12:30? Might give us time for one or two expanded sessions, and/or more time for freeform discussions between attendees ("networking")."* The program committee has taken this feedback into consideration and will continue to consider it during the planning of the 2017 summit.

A summary of the additional survey responses follows.

Forty-two attendees (approximately 42% of all attendees) responded to the general "Attendee Survey." The organizers did not submit responses, but the survey was open to all other participants. We did not request the names of respondents, and have redacted some information from the appended report to further protect the anonymity of respondents.

The quantified and categorical results (*e.g.*, rating scales, yes/no questions) were very favorable. Selections follow:

- To Question #5, "How would you rate your overall experience with the 2016 summit?," 98% of respondents selected "Good" or "Excellent."
- Regarding Question #7, "Was this summit better than what you expected, worse than what you expected, or about what you expected?," the summit at least met the expectations of 95% of respondents, exceeding the expectations of 60% of respondents.
- To Question #8, "How useful to your work was the information discussed at the summit?" 100% of respondents gave ratings of "moderately useful," "very useful," or "extremely useful," with 81% providing the higher two responses.
- To Question #9, "If you attended last year's summit, how does this year's compare?"

55% of respondents gave ratings of "this year's summit was about the same as last year's," "this year's summit was better than last year's," or "this year's summit was much better than last year's," with 32.5% providing the higher two responses. 42.5% of respondents indicated that they did not attend last year's summit.

- To Question #11, "Would you like to attend future summits?" 92.86% responded "Yes," with 4.76% responding "Maybe." Just one person, accounting for 2.38%, responded that they would not like to attend future summits.

Questions 13 and 14 sought open-ended responses, and were designed to elicit critique and discern highly-valued aspects of the experience. While the generally positive results of the above-referenced questions provide context, these open-ended questions have proved a useful communication tool. Observations follow:

- Question 13 asked, "How can we improve the summit experience in the future?" Of the 25 respondents to this question, 10 suggested some adjustments that would build on the current programming. An example response follows:

  > *"1. Hear more from students (poster sessions, lightening rounds, etc.) - this could be during coffee breaks. 2. Possibly make connections with students about summer REUs - this could be part of networking socials. 3. As a social scientist, I learned a lot about the infrastructure that's available for NSF research. However, I didn't have enough time to grasp everything. Perhaps a month before next year's summit, would it be possible to ask researchers to submit their current research projects (abstract) along with their corresponding infrastructure needs? And then ask infrastructure providers (ex. GENI, etc.) to see if there's any services that might be available to the researchers. Then, during the summit, pair up researchers with potential providers for 20 minutes. The researchers would (ideally) leave with specs sheets for provider services costs, logistics details, and cybersecurity considerations."*

- Question 14 asked, "Were there any aspects of the summit you found particularly useful or important? If so, please explain."

  - Of the 26 respondents, 8 praised the plenary discussions and 8 highlighted the training sessions as particularly useful or important.
  - Nine (9) respondents highlighted networking opportunities.

  An example response follows: *"The chance for members to present their solutions, and the candid discussion of the subject matter as well as the transparency in discussion and*

equal participation. This is really a community, rather than a canned presentation, and because of this, it's a unique conference."

6.2 Training Evaluation

The Training Day preceding this year's summit offered eight training sessions: 2 all day sessions, and 6 half day sessions. Each session was well attended, with topics and number of attendees as follows: Log Analysis Training with CTSC and Bro AM (14); Federated Identity Management for Research Organizations AM (6); REN-ISAC Cyberthreat Training (30 MinuteIntro) / Developing Cybersecurity Programs for NSF Projects (15); Building a NIST Risk Management Framework for HIPAA and FISMA Compliance (9); Secure Coding Practices and Automated Assessment Tools (7); Log Analysis Training with CTSC and Bro PM (11); Federated Identity Management for Research Organizations PM (7); Securing Legacy Industrial Control Systems (14); Building the Modern Research Data Portal Using the Globus Platform (8); and Secure Software Engineering Best Practices (14). Each tutorial attendee was asked to fill out a tutorial-specific survey after each training session concluded.

The responses to the tutorial-specific surveys were very positive generally, and included constructive feedback, as well as ideas for future training offerings. For simplicity, we asked attendees to complete one survey with several repeated questions to allow sorting differentiated responses for morning and afternoon sessions. The aggregated ratings in Questions 1 through 10, and 13 through 18 are attached as Appendix I. We summarize a few aggregate responses below:

- To Question 3, "Based on your overall experience with the August 16 training sessions, would you participate in training offered at future summits?," 22 (*i.e.*, 92%) of 24 respondents selected "Yes," 2 selected "Maybe," and 0 selected "No."
- To Questions 7 and 15, "How would you rate your overall experience with the [morning/afternoon] training?," 91% of responses were "Excellent" or "Good."
- To Questions 9 and 17, "Was this [morning/afternoon] training better than what you expected, worse than what you expected, or about what you expected?," 93% of responses indicated that expectations were met or exceeded. Forty-seven (47%) of responses were "Quite a bit better" or "A great deal better."
- To Questions 10 and 18, "How useful to your work was this [morning/afternoon] training?," 71% of responses were "Very Useful" or "Extremely Useful."

The responses for the individual tutorials were reported back to their respective tutorial leaders, including responses to Questions 11 and 19, "How can we improve this training session in the future?" and Questions 12 and 20, "Were there any aspects of [morning/afternoon]

training you found particularly useful or important? Please explain."

7 Progress Towards Priority Recommendations

The 2015 Summit defined a number of Priority Recommendations, Recommendations for Continued Action, and Opportunities and Recommendations for Exploration for future Summits. In this section we revisit those recommendations and discuss contributions to each made at the 2016 Summit.

7.1 Priority Recommendations

The following were identified by the 2015 summit as areas in need of focused attention.

7.1.1 Information Security Budgets

> **Recommendation 1:** The NSF CI and Large Facility community should develop a broadly applicable strategy for information security budgets, including how, why, and where it does what it does in terms of spending.

Discussion:

In 2015 budgets for information security emerged as a major theme and major question. This year a number of sessions touched upon funding information security efforts. Craig Jackson, Bob Cowles (CTSC) and Scott Russell (CACR), delivered a session specifically focused on security budgeting. Their research included the results of reviewing recent Cybersecurity spending surveys followed by a case study of DOE Science Labs security budgeting. Their research showed average security budgets lie between 3% to 12% of the IT budget. For our community they recommend engaging peer organizations to compare budgeting strategies. They also encouraged participation in the **2016 NSF Community Cybersecurity Benchmarking Survey** as a way for the CI community to aggregate information on the state of cybersecurity for NSF projects and facilities.

Other observations on security budgeting from the plenary:

- The keynote speaker, Peter Kuper from IQT presented a state of surging costs to secure assets despite a downward trend on return on investments - *"We are not winning the war"*. He suggest that organizations consider outsourcing services to commercial companies that have deep investments in their security operations.
- Chris Morrison (Gemini) & Tim Minick (HPM) cited a Forrester study showing security spending between 1-13% of IT budgets with 5.6% being the average.
- Irene Qualters (NSF) notes need for expert staff. A number of speakers commented that

attracting and retaining talent is challenging in the information security field.

- Abe Singer (NERSC) notes *"blocking ports and changing passwords costs time/money"*
- Tim Howard (NSF) shared the U.S. Antarctic Program information security budget is equal to 12.5% of the total IT budget.

There was a measurable increased interest in exploring funding security programs in 2016 that will continue in the coming years. The results of the community benchmarking survey could provide an interesting insights in 2017.

> **Recommendation 2**: The NSF CI and Large Facility community should support research on metrics that indicate whether spending on information security is sufficient and appropriately balanced with a project's science mission.

Discussion:

Several presentations discussed metrics for a cybersecurity program. Abe Singer's presentation on LIGO security qualitatively captured a cybersecurity goal well in the context of NSF science: *"LIGO [security] policy is to properly plan and implement security in a way that supports the scientific mission in a minimally intrusive manner that enables reliable access to data and use of LIGO."*

Other observations:

- Vic Thomas framed the goal of GENI cybersecurity in a manner that implied metrics: *"GENI seeks to build a trusted environment in which experimenters and resource owners can participate in resource allocation."* and *"These trust relationships reflect human/interorganizational relationships, nothing more."*
- Susan Ramsey of NCAR discussed the problem of too much policy resulting from a cybersecurity process being counterproductive.
- Warren Raquel of NCSA described the value of metrics as useful in justifying cybersecurity programs to management and identifying gaps.
- Tim Howard of the NSF Polar Program noted the need to *"Continually evaluate IT investment to balance security investments against operational investments"* with the context that our goal is to *"do science, securely."*
- Michael Sinatra's presentation on Science DMZs stressed the need for risk-based security and the goal of transmitting science data.

Taken together, these observations reflect a growing consensus that cybersecurity exists to produce more secure science and that metrics for cybersecurity in the context of open science should include the impact on science (the smaller the impact the better).

7.1.2 Accountability, Risk Acceptance, and the Role of Project Leadership

> **Recommendation 3**: The NSF CI and Large Facility community should develop a common understanding among all stakeholders of how accountability, risk responsibility, and risk acceptance practices are most efficiently and appropriately distributed among project leadership, project personnel, and other stakeholders.

Discussion:

The role of project leadership continued as a theme across many plenary sessions. Susan Ramsey (NCAR) discussed the importance of getting executive sponsorship when developing/maturing an information security program. This includes having the executive/senior project management involved in the risk management process along with signatory acceptance of the audit findings and other official documents.

Additional discussions on risk responsibility and accountability from the plenary:

- Abe Singer (former LIGO CISO) discussed LIGO's security program that includes a team of stakeholders that identify risks and mitigation controls along with residual risk. A report containing this information is presented to the Directorate management for official sign-off.
- Vicraj Thomas described how security responsibilities are shared among the GENI federation. GENI uses a number of Federation agreements to outline responsibilities including those of Aggregate providers, Clearinghouse providers, and an acceptable use policy.

7.1.3 Requirements for Software Assurance, Quality, and Supply Chain

> **Recommendation 4:** The NSF CI and Large Facility community should determine its software assurance, quality, and supply chain requirements.

Discussion:

Software assurance was a point of emphasis in 2015, with featured talks by Dave Nalley, *The Tragedy of Open Source,* and Amar Takhar, *Risks of Infrastructure Neglect and the Road Ahead*, focusing a detailed discussion on challenges to open source software maintenance as they pertain to security. In 2016, we noted software reviews are part of LIGO's cybersecurity program (as reported in Abe Singer's talk), and the software security training continues to be well-attended, but there was not otherwise a strong response to this topic from the community.

It is the observation of the organizers that this topic is not one that many operational

cybersecurity people feel expert in and it has a steep learning curve, which makes it challenging to incorporate into cybersecurity programs and hence may reflect its lack of representation in presentations. Requests to CTSC for engagements focusing on software security would seem to support this. With the recently funded NSF Software Institutes, we suggest engagement and coordination with NSF projects to determine their goals regarding software security may yield some unmet requirements in this space.

7.2 Recommendations for Continued Action

The 2015 summit report highlighted a handful of areas for continued work. These are areas where there is evidence that progress is being made, but must continue. These not as urgent as the recommendations in Section 7.1, and were not a focus of the 2016 summit, but we note any related discussion.

7.2.1 Baseline Expectations

> **Recommendation 5*:*** Utilizing a consensus process that includes all stakeholders, the NSF CI and Large Facility community should adopt a common, broadly applicable framework for information security.

*Discussion***:**

The 2016 summit included a presentation from Tim Howard of NSF's Division of Polar Programs on "Strengthening Trustworthy Science: Ideas for Adapting the NIST Risk Management Framework to the NSF Cooperative Agreement for Large Facilities." This presentation discussed the use of project-based risk management to cybersecurity with the observation "We are already doing the Risk Management Framework, might as well claim credit for it." and suggests "If we as the cybersecurity expertise for cyberinfrastructure evaluate the NIST Risk Management Framework more thoroughly, we can define standard approaches for adapting the RMF to unique science mission programs."

7.2.2 Risk-Based Approaches

> **Recommendation 6:** The NSF CI and Large Facility community should continue to implement, refine, and evaluate risk-based approaches to cybersecurity that leverage established best practices as much as possible, while also addressing the community's particular needs around unique scientific instruments, data, openness, multi-organizational relationships, mission assurance, resilience, and project lifespans.

Discussion:

The presentations from LIGO, TACC, Gemini, GENI all highlight individual approaches to

cybersecurity and include risk-based approaches. The presentation on Science DMZs highlight them as a risk-based approach to enabling scientific data transfer through network segmentation.

The discussion of metrics (see Section 7.1.1) highlights many of the community's particular needs around unique science assets as does the Open Science Cyber Threat (Risk) Profile discussed in the Cybersecurity Center of Excellence update.

7.2.3 Community Building & Information Sharing

> **Recommendation 7:** The NSF CI and Large Facility community should find more ongoing ways of collaboratively developing and maintaining cybersecurity programs, such as sharing materials, services, practices, lessons learned, and collaborative/peer reviews.

Discussion:

This summit continued a dramatic increase in the open discussion of projects' and facilities' specific information security practices and lessons learned, with CFP responses driving the majority of the agenda. There was some discussion on how we could foster increased sharing of incidents and "lessons learned" in addition to success stories and the organizers agree that continuing to work on social factors to increases attendee's comfort level with share should continue to be a focus.

7.2.4 Identity and Access Management

> **Recommendation 8:** The NSF CI and Large Facility community should continue to develop and disseminate best practices for identity and access management to support research.

Discussion:

In addition to a repeat of the "Federated Identity Management for Research Organizations" training, there was a presentation from FermiLab on "Computing Grid Access with Federated Identity" at the 2016 summit. This presentation provided an update on identity management in the Open Science Grid and its use of CILogon.

7.3 Opportunities for Exploration

The 2015 summit identified areas of opportunity, which the community may want to exploration to identify the magnitude or benefit or risk associated with each area. As with the prior Recommendations for Continued Action, these were not a focus of the 2016 summit nor are they considered to critical areas in need of immediate attention. We include them in the

report to note note any related discussion. Some current opportunities may evolve to become future community recommendations if interest increases.

7.3.1 NSF-Funding Facilities and Projects as Real-World Cybersecurity Research Environments

> **Opportunity 1[12]:** The NSF CI and Large Facility community should explore how it can support, participate in, and directly benefit from basic and applied cybersecurity research like that funded via NSF's Secure and Trustworthy Cyberspace (SaTC) and Risk and Resilience solicitations.

Discussion:

As a result of the call for participation, Dr. Ragib Hasan presented on "Provenance Based Security" research at the 2016 summit. Additionally, several project presentations, notably GENI and OSG, described security architectures which could be described as applied research. In particular Vic Thomas described how GENI is used for research and education in cybersecurity topics such as: DDoS mitigation using SDN; OpenFlow based firewalls and NATs; Man-in-the-middle attacks; and ToR networks.

7.3.2 Community Threat Model

> **Opportunity 2[13]:** The NSF CI and Large Facility community should closely follow, participate in, evaluate, and validate the NSF Cybersecurity Center of Excellence's community threat model development effort, including determining whether insights into threat actors and threat events positively impact the efficiency and effectiveness of our cybersecurity programs and risk management processes.

Discussion:

As highlighted in Welch's talk on the activities by the Cybersecurity Center of Excellence, it has collaborated with ESnet to assemble a working group to develop a Risk Profile which describes common scientific assets and how they can be impacted by threats. Subsequent to the summit, the working group has released the initial version of this profile at http://trustedci.org/oscrp/.

7.3.3 Real Time Data, Threat Intelligence, and Information Sharing Services

[12] Previously Recommendation 10 in 2015
[13] Previously Recommendation 11 in 2015

Opportunity 3[14]: The NSF CI and Large Facility community should explore collaboration with, and even drive change in, existing cross-organizational mechanisms (*e.g.*, REN-ISAC, EDUCAUSE, Internet2) where information sharing can efficiently and effectively help the community gain a defensive advantage.

Discussion:

The presentation on the Cybersecurity Center of Excellence described its new situational awareness service (http://trustedci.org/situational-awareness/).

7.3.4 Privacy

Opportunity 4[15]: The NSF CI and Large Facility community should determine when and how privacy intersects with NSF CI cybersecurity efforts in terms of (i) legal and regulatory requirements; (ii) our community's norms, values, and stakeholder relationships; and (iii) being a barrier to and/or enabler of science.

Discussion:

Tim Howard's presentation noted requirements for privacy based on FISMA, OMB Circular A-130, and NSF's Proposal and Award Policies and Procedures Guide (PAPPG) guidance on Data Management Plans.

This report shifts Privacy from a Recommendation of Continued Action, where it was listed in 2015, to a Opportunity for Exploration due to a perceived lack of ongoing effort in this area.

8 Closing Thoughts from the Organizers

We continue to be extremely happy with the impact the summit is having in terms of bringing the community together, soliciting responses to the call for participation, and fostering sharing experiences amongst the community. We thank the community members who enable this success through their participation at the summit. In particular we thank those who serve on the program committee. We're excited to see a second year of growth in community participation and response to the call for proposals, again exceeding the program's capacity to accommodate.

We do believe however that we, the program committee, and the community should not become complacent. With our established trust and sense of community, we should consider and continue to refine our ongoing and long-term goals to ensure we continue our current

[14] Previously Recommendation 12 in 2015
[15] Previously Recommendation 9 in 2015

successes and continue to produce new successes as well as adapt to changes in the cybersecurity and NSF landscapes. We will continue to evolve the summit to adjust to meet the community's changing needs.

We will continue to adjust our registration scheme to obtain fair participation by the NSF and broader communities - e.g. modeling what we have seen at other NSF PI meetings, we are considering allowing each NSF project to have two free attendees and charge for additional attendees or those not from an NSF project or with an invitation from the organizers.

Finally, we thank the program committee members for their hard work and devotion to the summit, and we thank NSF for funding the summits and providing presentations.

-2016 Summit Organizers: Jim Basney, Ryan Kiser, Jim Marsteller, Susan Sons, Amy Starzynski Coddens, and Von Welch.

Appendix A
The Agenda

Program Agenda

2016 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

August 16 - August 18 Westin Arlington Gateway Arlington, Virginia

http://trustedci.org/2016summit

Updated August 17, 2016

PC: Steve Barnet, Tony Baylis, Mike Corn, Barb Fossum, Ardoth Hassler, Susan Ramsey, George Strawn

Organizers: Leslee Cooper, Ryan Kiser, Jim Marsteller, Susan Sons, Jim Basney, Amy Starzynski Coddens, Von Welch

---

Training Day

Tuesday, August 16, 2016

http://trustedci.org/2016training/

8:00am Registration and Continental Breakfast (Pre-Function Hemingway)

9:00am Morning and All Day Training Sessions Begin

- Log Analysis Training with CTSC and Bro
- Federated Identity Management for Research Organizations
- REN-ISAC Cyberthreat Training (30 Minute Intro) / Developing Cybersecurity Programs for NSF Projects
- Building a NIST Risk Management Framework for HIPAA and FISMA Compliance
- Secure Coding Practices and Automated Assessment Tools

11:00am *Coffee Break*

11:30am Training Sessions Resume

1:00pm *Lunch provided*

2:00pm Afternoon Training Sessions Begin and All Day Training Sessions Resume

- Log Analysis Training with CTSC and Bro
- Federated Identity Management for Research Organizations
- Securing Legacy Industrial Control Systems
- Building the Modern Research Data Portal Using the Globus Platform
- Secure Software Engineering Best Practices

4:00pm *Coffee Break*

4:30pm Training Sessions Resume

6:00pm Sessions End

Evening: *Dinner on your own*

Plenary Session

Wednesday, August 17, 2016
F. Scott Fitzgerald AB

8:00am	Sign-In and Continental Breakfast (Pre-Function AB)
9:00am	Welcome and Goals (Jim Marsteller)
9:10am	NSF Address: Irene Qualters, Division Director: ACI
9:30am	Keynote Address: Peter Kuper
10:30am	NSF Cybersecurity Center of Excellence (Von Welch)
11:00am	*Coffee Break*
11:30am	Security at the Texas Advanced Computing Center (Nathaniel Mendoza, Patrick Storm)
12:00pm	Gemini Observatory Cybersecurity Program (Chris Morrison, Tim Minick)
12:30pm	Security at LIGO (Abe Singer)
1:00pm	Lunch and Table Topics - *Lunch provided*
2:30pm	The Science DMZ as a Security Architecture (Michael Sinatra)
3:00pm	Cybersecurity Budgeting (Scott Russell, Craig Jackson, Bob Cowles)
3:30pm	Provenance Based Security: Toward Building Provenance-Aware Secure Systems (Ragib Hasan)
4:00pm	*Coffee Break*
4:30pm	Computing Grid Access with Federated Identity (Mine Altunay, Dave Dykstra)
5:00pm	Using Globus Authorization to Streamline the Creation, Integration, and Use of Research Services (Ian Foster, Lee Liming, Steve Tuecke)
5:30pm	Open Discussion / Summary of the Day's Findings (Jim Marsteller / Von Welch)
6:00pm	Dismissal
Evening:	*Dinner on your own.* *Informal Dinner Gathering at TBD*

Plenary Session (continued)

Thursday, August 18, 2016
F. Scott Fitzgerald AB

8:00am	Sign-In and Continental Breakfast (Pre-Function AB)
8:50am	Welcome Back (Jim Marsteller)
9:00am	Panel: "FBI Case 216 Retrospective Panel" Moderator: Jamie Allan, Program Director - Ocean Drilling Program, NSF Panelists: RuthAnne Bevier (Caltech) Clifford Jacobs (Clifford A. Jacobs Consulting, LLC) Victor Hazlewood (University of Tennessee) Adam Slagell (NCSA)
10:00am	GENI Cybersecurity: Mechanism, Policies and Procedures (Vicraj Thomas)
10:30am	Strengthening Trustworthy Science: Ideas for Adapting NIST Risk Management Framework to the NSF Cooperative Agreement for Large Facilities (Tim Howard, Steve Barnet)
11:00am	*Coffee Break*
11:30am	Compliance Panel: FISMA, FERPA, and HIPAA, Oh My! (Susan Ramsey, Anurag Shankar)
12:00pm	Open Discussion / Summary of Summit Findings (Von Welch, Jim Marsteller)
12:30pm	Adjourn

Appendix B
Biographies for Speakers, Program Committee, and Organizers

2016 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

Bios for Speakers, Authors, Program Committee Members, Organizers, and Student Awardees

---

In alphabetical order by surname

Mine Altunay is a computer science researcher focusing on information security. At Fermilab, she is responsible for ensuring scientific infrastructure meet the laboratory's security requirements and provide a secure and convenient environment for our scientists. In addition to her role at Fermilab, she is responsible for security of the worldwide CMS collaboration and also act as the OSG Security Officer. She has a PhD in information security from North Carolina State University. Her main research focus has been on identity management in distributed collaborative environments such as cloud computing. In the past, she was a research fellow at IBM Research at Tokyo Japan, and was a member of IBM Extreme Blue team and IBM HiPODS teams.

*

Steve Barnet has specialized in supporting scientific and academic computing for nearly 20 years. During that time, he has worked in multiple domains including storage, networking, high-throughput computing, and security. He handled his first incident in 1995, a compromised Solaris system providing several important infrastructure services.

Steve currently works for the IceCube project, a kilometer scale neutrino detector located at the geographic South Pole. He began collaborating with CTSC in 2013 to develop a Cybersecurity plan for the IceCube facility.

*

Dr. Jim Basney is a senior research scientist in the cybersecurity group at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign. Jim's area of expertise is identity management for scientific collaborations. He is PI of the CILogon project and co-PI of the Center for Trustworthy Scientific Cyberinfrastructure, FeduShare, and Software Assurance Marketplace projects. Jim also contributes to the LIGO, LSST, and XSEDE projects. He received his PhD in computer sciences from the University of Wisconsin-Madison.

*

Tony Baylis of Lawrence Livermore National Laboratory is the Laboratory's Director for the Office of Strategic Diversity and Inclusion Programs. In this position, he is the senior management advocate for diversity and inclusion for the Laboratory. The Office of Strategic Diversity and Inclusion Programs partners with senior management to develop strategies, initiatives, programs, and activities that promote the creation of a diverse and inclusive workforce and work environment. Tony serves as the Laboratory's EEO, AA and Diversity compliance officer as well. In conjunction with these tasks, Tony is responsible for overseeing the laboratory's interactions and successful execution in building, partnering and collaborating with governmental, educational, industrial, community interests and other stakeholders. LLNL has had a long history in working with Minority Serving Institutions, specifically relationships with American Indian Institutions, Hispanic Institutions and Historically Black College and Universities. He represents the Laboratory on the subjects of Diversity and Inclusion,

STEM, Outreach Efforts, and Student Programs.

Tony's career represents 26 years of administrative, project, program, technical and organizational management. He has worked in a scientific and technical environment for over 20 years and has worked as an consultant in industry as well. Tony has extensive experience networking with a broad range of academic, industry, government and non-profit organizations that has educated him and helped him in his career. He serves on a number of conference program committees and advisory boards that promote STEM and diversity in science and technical careers. He has been an NSF reviewer and PI/Co-Pi for the Broadening Participation in Computing Program. Tony is also an ACM and ACM SIGGRAPH member, and serves as the Treasurer for ACM SIGGRAPH. He is a graduate of the University of Illinois.

*

RuthAnne Bevier, is the Chief Information Security Officer at the California Institute of Technology. She joined Caltech in 1996, and has worked in Information Security there since 1999. In 2004 she served on the program committee for the first of what became the NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure. More recently she served as a reviewer for the 2104 National Academies publication, _At The Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.

RuthAnne received her Master's degree in Library and Information Science from the University of California, Berkeley.

*

Leslee A. Cooper serves as the Administrative & Finance Director at Indiana University's Center for Applied Cybersecurity Research (CACR). She is a graduate of the IU School of Business (B.S. '93). Leslee comes to the CACR and CTSC from a background in Management, Finance and Accounting. She has worked with government divisions, as well as in the private sector.

*

Michael Corn is the Deputy CIO and CISO for Brandeis University. His areas of interest include privacy, identity management, and cloud services. He has been an active speaker and author on security and privacy and has participated in numerous Educause and Internet2 initiatives. He is a member of the Internet2 Netplus Product Advisory Board and until recently was also a member of the Box.com and Splunk Product Advisory Boards, as well as the Kuali Ready Product Board.

Prior to joining Brandeis he was the CISO and Chief Privacy and Security Officer of the University of Illinois at Urbana-Champaign. He is a graduate of the University of Colorado at Boulder and the University of Illinois at Urbana-Champaign.

*

Robert (Bob) Cowles is principal in BrightLite Information Security performing cybersecurity assessments and consulting in research and education about information security and identity management. He served as CISO at SLAC National Accelerator Laboratory (1997-2012); participated in security policy development for LHC Computing Grid (2001-2008); and was an instructor at University of Hong Kong in information security (2000-2003).

*

Dominique Dalanni is a junior at California State University, Dominguez Hills where she is pursuing a Bachelor's of Science in Computer Science. In addition to her studies, Ms. Dalanni is currently the president of the Women in Stem Club, vice president and student advocate for the Computing Alliance of Hispanic Serving Institutions (CAHSI) Club CSUDH chapter, and secretary of the Cybersecurity Club at her university. She also serves as a research assistant in a project funded by the Nuclear Regulatory Commission and in 2015 was selected to represent her university as a CSU Trustee Award recipient and scholar.

After completing her undergraduate education, Ms. Dalanni hopes to pursue a graduate degree at George Washington University in Computer Science with a specialization in Cybersecurity. Once she has received her graduate degree, Ms. Dalanni would like explore job opportunities which focus on threat analysis, governance, or on the overall security of industrial control systems.

*

Jeannette Dopheide is an education outreach coordinator at NCSA. Her experience in education and outreach began as a high school teacher before moving onto business systems analysis and applications training for a commercial software company. Jeannette joined CTSC and NCSA in 2014 and works primarily on education outreach for projects that impact both CTSC and NCSA, including the Bro Project. Jeannette is a graduate of Illinois State University.

*

Dave Dykstra received his PhD in Computer Science from the University of Illinois at Urbana-Champaign. For the first part of his career he worked for AT&T and Lucent, where he was best known for being the leader of the Exptools project that distributed software binaries to developers throughout the company, mostly open source software. During that time he also led the open source rsync project for a year. For the past 10 years he has been at Fermilab where his primary duties have been supporting the Frontier Distributed Database system for CMS and ATLAS, the Worldwide LHC Computing Grid's squid web proxy caching network, and the Open Science Grid's installation of the CernVM Filesystem, and also doing security research for the Open Science Grid.

*

Vitaly Ford is a 5th year doctoral student in Computer Science at Tennessee Tech University. His research areas include privacy and information security in the Smart Grid as well as cybersecurity education. He is one of the founders and an advisor for CyberEagles cybersecurity club at Tennessee Tech. Vitaly promotes cybersecurity education and training among students at the National Cybersecurity Student Association as an Advisory Board member. His dissertation topic is about developing an efficient privacy-preserving advanced metering infrastructure supporting fine-grained data analysis. In his free time, Vitaly enjoys playing table tennis and chess as well as participating in Capture The Flag cybersecurity competitions. His career goal is to become a faculty member after graduation.

*

Barbara Fossum is a senior executive with over 25 years of leadership and management experience in higher academic and government sectors including high performance computing, data visualization, engineering and academic research. Barbara contributed several federally funded grants including the

Network for Engineering Simulations where she successfully directed all operations and the development of a curated data repository for all earthquake engineering data. She is currently the CEO of BMF Consulting, providing extensive experience in human resource planning and operations, organizational change, team building, organizational effectiveness and facilitative leadership.

*

Ian Foster is a Professor of Computer Science at the University of Chicago and a Senior Scientist and Distinguished Fellow at Argonne National Laboratory. Originally from New Zealand, he has lived in Chicago for longer than he likes to admit. Ian has a long record of research contributions in high-performance computing, distributed systems, and data-driven discovery. He has also led US and international projects that have produced widely used software systems and scientific computing infrastructures. He has published hundreds of scientific papers and six books on these and other topics. Ian is an elected fellow of the American Association for the Advancement of Science, the Association for Computing Machinery, and the British Computer Society. His awards include the British Computer Society's Lovelace Medal and the IEEE Tsutomu Kanai award.

*

Nikita Golubets is a student majoring in Information Assurance & Cyber Defense with a main focus in Network Security/Administration at Eastern Michigan University. He enjoys taking part in Information Security competitions such as ISTS (The Information Security Talent Search) and CCDC (National Collegiate Cyber Defense Competition). After graduation, he would like to obtain a position that will allow him to gain experience in either malware analysis or system administration.

*

Vlad Grigorescu is a Security Engineer for the Incident Response and Security team at the National Center for Supercomputing Applications. Vlad is also a core developer on The Bro Project. In addition to his work on Bro he is the creator and developer of Brownian, a web interface for interacting with Bro logs. Vlad earned a B.S. in computer engineering from the University of Illinois at Urbana-Champaign.

*

Ragib Hasan, Ph.D., is a tenure-track Assistant Professor at the Department of Computer and Information Sciences at the University of Alabama at Birmingham.

Hasan explores research on cloud security, the Internet of Things, digital forensics, mobile malware security, secure provenance, biomedical device security, social network security, and database security. Hasan is the founder of the Secure and Trustworthy Computing Lab (SECRETLab) at UAB. He is also a member of the UAB Center for Information Assurance and Joint Forensics Research and a member of the NIST Working group on Cloud Forensics.

Prior to joining UAB, He received his Ph.D. and M.S. in Computer Science from the University of Illinois at Urbana Champaign in October, 2009, and December, 2005, respectively, and was an NSF/CRA Computing Innovation Fellow post-doc at the Department of Computer Science, Johns Hopkins University.

Dr. Hasan's research is supported by the Department of Homeland Security, the Office of Naval Research, the National Science Foundation, Facebook Inc., Google Inc., and Amazon Inc. He is a 2014

awardee of the prestigious NSF CAREER Award from the National Science Foundation for his work on cloud security. Dr. Hasan is also a recipient of the 2015 mBillionth Award for m-learning, the 2013 Google RISE Award, a 2013 Information Society Innovation Fund Award. 2014 Deutsche-Welle Best of Blogs and Online Innovation award for his BanglaBraille project, a 2011 Google Faculty Research Award, the 2009 NSF Computing Innovation Fellowship and the 2003 Chancellor Award and Gold Medal from Bangladesh University of Engineering and Technology. He is a founding member of Wikimedia Bangladesh chapter, a long term administrator of Bangla and English Wikipedias, and also the founder of Shikkhok.com – an award-winning online education platform for advancing STEM education in rural areas of India and Bangladesh which has won the 2013 Google RISE Award and 2013 Information Society Innovation Fund Award.

*

Ardoth Hassler is Associate Vice President of University Information Services at Georgetown University. Her work focuses on policy, planning and research, including being the PI for NSF CC-NIE and CC-IIE awards. In addition, she is Interim Director of the Student Information Systems group. Ardoth was on loan to the National Science Foundation 2007-2011 where she served as Senior Information Technology Advisor in the Office of the Chief Information Officer in the NSF Office of Information and Resource Management, Division of Information Systems. Her activities included work related to cybersecurity best practices for large research facilities, working on technology policy for the Foundation and large research facilities, assisting NSF in joining the InCommon Federation and introducing concepts of single-sign-on logon to Research.gov, leading the "SSN Be Gone" project to remove SSNs from FastLane and other systems where there was no business need, working on NSF's "Got Green", initiative, etc. She has prior experience serving on the program committees of the NSF Cybersecurity Summit, EDUCAUSE Annual Conferences, etc. She has a BS in Math (CS minor) from Oklahoma State University and an MS in Biostatistics from the University of Oklahoma.

*

Victor Hazlewood is the Chief Operating Officer of the Joint Institute for Computational Sciences (JICS) at the University of Tennessee responsible for Networking, Security and Operations with over 27 years of experience in High Performance Computing (HPC) in the research community. Victor has extensive security knowledge and experience in the academic research environment including participation in the TeraGrid and XSEDE Incident Response program and participation in the community response to the 2004-2005 Stakkato incident. Victor is currently the Deputy Director of Operations for XSEDE and is PI on the UT portion of the NSF collaborative award for the DANCES software defined networking project (http://www.dances-sdn.org/).

*

Randy Heiland is a Senior Systems Analyst/Programmer at IU's Center for Applied Cybersecurity Research. He has spent most of his career developing software for a wide range of science and engineering disciplines - in industry, government labs, and academia. Since 2013, he has been part of the NSF CTSC project (trustedci.org) and contributed to several engagements (trustedci.org/engagements). He has broad interests in mathematics and science and enjoys sharing those passions with young people. (MS/Computer Science, U. Utah; MA/Mathematics, Arizona State U.)

*

Todd Herring is the Membership Services Director for REN-ISAC. He has worked as an IT professional for Indiana University, in one capacity or another, for over 20 years, cutting his teeth in a Novell world with command prompts and minuscule amounts of memory and disk compared to today. He became more deeply focused on security back in the early 2000s, when it became apparent that unprotected systems could be compromised in a matter of minutes. As a network systems admin, he was responsible for securing servers and workstations; configuring solid computer builds; configuring firewalls, IPSec, and group policy objects; and documenting procedures and change management activities. More recently, Mr. Herring has been involved with IT security compliance as part of an enterprise risk management project at IU. His role at REN-ISAC is focused on membership and partner relationships, leading projects geared toward improved services.

*

Elisa Heymann is a Senior Scientist at the Computer Sciences Department of the University of Wisconsin-Madison, and an Associate Professor in the Computer Architecture and Operating Systems Department at the Autonomous University of Barcelona (UAB). She co-directs the MIST software vulnerability assessment project in collaboration with her colleagues at the University of Wisconsin.

Heymann is part of CTSC, the NFS cyber security center for excellence, where she works on Software Assurance training and engagements. Heymann carries out training in universities, companies, and conferences around the world.

Heymann's research interests include security and resource management for Grid and Cloud environments, and cyber-security in transportation. Her research is supported by NSF, the Spanish government, the European Commission, and NATO.

Heymann received her M.S. and Ph.D. degrees in Computer Science from the Autonomous University of Barcelona (Spain) in 1995 and 2001 respectively.

*

Tim Howard is the Information Technology Operations and Security Program Manager for the National Science Foundation U.S. Antarctic Program (USAP). Tim oversees the IT infrastructure operations and cybersecurity activities at 11 USAP operating locations, including three Antarctic research stations and two research vessels. Each year, the USAP IT infrastructure supports 118 science and technical events conducted by 72 academic institutions and federal agencies across eight major science program areas, including the IceCube Neutrino Array and the South Pole telescope. Prior to his arrival at NSF, Tim served as the Information Security Team Lead for NOAA's weather satellites, which included an assignment to the NOAA-NASA team that successfully refurbished the Deep Space Climate Observatory, which launched in February 2015 and is now orbiting the Sun-Earth L-1 libration point, where it collects solar winds measurements to help the National Weather Service provide early warning space weather forecasts to the energy, telecommunications, and other critical infrastructure sectors. Tim is a Certified Information System Security Professional (CISSP), and a Penn State grad with a Bachelor of Science degree in Aerospace Engineering. Tim also holds a Master of Science degree in Telecommunications Management from the University of Maryland University College and is currently participating in the Chief Information Officer certificate program at Carnegie-Mellon University.

*

Craig Jackson is Chief Policy Analyst at Indiana University's Center for Applied Cybersecurity Research (CACR), where his research interests include risk management, information security program development and governance, legal and regulatory regimes' impact on information security, and identity management. He is a co-PI for the Center for Trustworthy Scientific Cyberinfrastructure (CTSC); he is a member of the security team for the DHS-funded Software Assurance Marketplace (SWAMP); and he is part of the DOE-funded XSIM (Extreme Scale Identity Management) project. He is a graduate of the IU Maurer School of Law (J.D.'10) and IU School of Education (M.S.'04). As a member of the Indiana bar, Mr. Jackson has represented government and corporate clients in constitutional and tort claims. His research, design, and project management background includes work at IU School of Education's Center for Research on Learning and Technology and Washington University in St. Louis School of Medicine. He is a member of Phi Beta Kappa, and was a Lien Honorary Scholar at Washington University in St. Louis.

*

Deja T. Jackson is an undergraduate at Kennesaw State University pursuing a degree in Computer Science. After receiving the National Center for Women in Technology Georgia award in 2015, she has been inspired to help and foster interest in computing within others; therefore has immersed herself in a variety of leadership positions including Student Government Senator for the College of Computing, and Vice-President of Object-Oriented Owls, a program designed to support women in computing. She has also been active in numerous research opportunities including the Louis Stokes Alliance for Minority Participation and the Georgia Tech Undergraduate research program, both funded by the NSF. Upon graduation, Deja hopes to use her experience and knowledge to land a career in cyber security within the private sector.

*

Rasib Khan, Ph.D., is an Assistant Professor of Cybersecurity in the department of Computer Science at Northern Kentucky University (NKU). Khan received his Ph.D. in Computer and Information Sciences from University of Alabama at Birmingham (UAB) in 2016. He worked in the SECuRE and Trustworthy computing Lab (SECRETLab) at the Center for Information Assurance and Joint Forensics Research (The Center) at UAB while working on his research on secure service frameworks, information provenance, authentication and authorization in cloud, distributed, and decentralized systems. He served as the lead researcher at SECRETLab for the Department of Homeland Security funded project on secure location provenance for mobile devices. Khan was a NordSecMob European Union Erasmus Mundus Scholar, and received dual MS degrees in Security and Mobile Computing from Royal Institute of Technology (KTH), Sweden, and Aalto University (formerly Helsinki University of Technology), Finland in 2011. Khan also worked as the security researcher in the European Union FP7 PURSUIT project while working at Helsinki Institute for Information Technology (HIIT), Finland, from 2011 till before moving to the US in 2012. Prior to joining HIIT, he worked in the Cloud Security group at Nomadic Lab, Ericsson Research, Finland, where he worked on decentralized authentication systems and cloud computing frameworks.

*

Ryan Kiser, IT Specialist, Center for Applied Cybersecurity Research

*

Scott Koranda, PhD, specializes on identity management architecture for research organizations. Since 2008, Scott Koranda has designed, deployed, and supported production SAML infrastructures

including both the Shibboleth Identity Provider (IdP) and Service Provider (SP) software, for the research and education sectors.

A member of the Laser Interferometer Gravitational-Wave Observatory (LIGO) collaboration for over 10 years, Scott has served as the lead architect for the LIGO Identity and Access Management project since 2007. He was co-principal investigator on the NSF grant that funds COmanage development, and is a consultant with Spherical Cow Group.

*

Peter Kuper is a Partner with In-Q-Tel, the nonprofit strategic investment firm that identifies, adapts, and delivers innovative technologies to support the missions of the U.S. Intelligence Community. Peter actively seeks and works with private companies with a particular focus on security and enterprise software. Previously, Peter was the lead software analyst for Morgan Stanley where he published industry leading investment reports and led over 18 public transactions.

Peter was a Wall Street analyst for 15 years offering him the opportunity to work with some of the most dynamic and talented public and private companies and the world's leading investment professionals. As a visible voice for the software industry, Peter has given numerous presentations to professional and government groups and has been interviewed on CNBC, Bloomberg Television, and quoted in most leading publications including *The Wall Street Journal* and *The Financial Times*. He has also published articles in *IEEE Magazine*. Peter currently serves as an adviser to the Pacific Northwest National Lab and is a Faculty member for IANS.

*

Lee Liming is a Technical Communications Manager at the Computation Institute, a joint venture between The University of Chicago and Argonne National Laboratory. He has spent sixteen years working with scientists from many fields of study to build computing systems capable of supporting their ever-growing data and computing needs. Past collaborations have included civil engineers, space scientists and astronomers, climate scientists, high-energy physicists, energy scientists, cosmologists, social scientists and librarians, neuroscientists, cancer researchers, and, of course, computer scientists. Prior to working at the University of Chicago and Argonne, Lee was a Sr. Product Manager and Principle Engineer at ProQuest Information and Learning and an information technology manager at the University of Michigan. Lee received a B.S.E degree in Computer Engineering at the University of Michigan.

*

James A. Marsteller, Jr. (CISSP) is the Chief Information Security Officer of the Pittsburgh Supercomputing Center,where he is responsible for ensuring the availability and integrity of the PSC's high performance computing assets. Jim has over 16 years experience in the information security field and more than 25 years of professional experience in the field of technology. He also serves as a member of the board for the Pittsburgh Infragard Chapter. Prior to working at PSC, he was a program manager for the Carnegie Mellon Research Institute that provided information security consulting services for government agencies and Fortune 500 companies. Jim co-leads the XSEDE Incident Response team and is XSEDE's security officer. He is a Co-PI for the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). Jim has served as the program chair the Cybersecurity Summit since 2009.

*

Nathaniel Mendoza is Chief Security Officer and Senior Network Administrator at the University Of Texas Austin's, Texas Advanced Computing Center (TACC) where he leads a group of the Security, Network, and Systems Administrators. Current areas of work include Cloud Computing, High Speed Networks, Operational Security, and Compliance. Additionally, he is a part of the XSEDE security group and has been a member of Super Computing's SCInet. Previous to joining TACC in 2011 he was the Chief Security Officer and Senior Network Engineer at the University of Tennessee Knoxville's, National Institute for Computational Sciences (NICS).

*

Kim Milford is the Executive Director of REN-ISAC. Under Executive Director Milford's oversight, REN-ISAC provides research and education institutions with services that facilitate better information security and leads REN-ISAC operations, hosted at Indiana University. She joined Indiana University in 2007 and served in leading strategic IT initiatives, directing the work of the University Information Policy Office, and as the Chief Privacy Officer.

Previously, Milford served as the Information Security Officer at the University of Rochester, where she led a comprehensive information security program. As Information Security Manager at University of Wisconsin-Madison, she co-led the establishment of the university's information security department. Millford has a J.D. from John Marshall and a B.S. in Accounting from St Louis University.

*

Barton Miller is Professor of Computer Sciences at the University of Wisconsin. He is Chief Scientist for the DHS Software Assurance Marketplace research facility. He co-directs the MIST software vulnerability assessment project in collaboration with his colleagues at the Autonomous University of Barcelona. He also leads Paradyn Parallel Performance Tool project, which is investigating performance and instrumentation technologies for parallel and distributed applications and systems. His research interests include systems security, binary and malicious code analysis and instrumentation extreme scale systems, parallel and distributed program measurement and debugging, and mobile computing. Miller's research is supported by the U.S. Department of Homeland Security, U.S. Department of Energy, National Science Foundation, NATO, and various corporations.

In 1988, Miller founded the field of Fuzz random software testing, which is the foundation of many security and software engineering disciplines. In 1992, Miller (working with his then-student, Prof. Jeffrey Hollingsworth, founded the field of dynamic binary code instrumentation and coined the term "dynamic instrumentation". Dynamic instrumentation forms the basis for his current efforts in malware analysis and instrumentation.

Miller was the chair of the IDA Center for Computing Sciences Program Review Committee, a member of the Los Alamos National Laboratory Computing, Communications and Networking Division Review Committee, and has been on the U.S. Secret Service
Electronic Crimes Task Force (Chicago Area), the Advisory Committee for Tuskegee University's High Performance Computing Program, and the Advisory Board for the International Summer Institute on Parallel Computer Architectures, Languages, and
Algorithms in Prague. Miller is an active participant in the European Union APART performance tools initiative.

Miller received his Ph.D. degree in Computer Science from the University of California, Berkeley in 1984. He is a Fellow of the ACM.

*

Tim Minick is the Director of Information Technology for HPM Building Supply, an employee owned retailer, manufacturer, and building materials company with branches across the Hawaiian Islands. In the decade prior to joining HPM Tim worked at AURA/Gemini Observatory, relocating to Hawaii from the U.S. mainland in 2005. Beginning in 2010 Tim managed the Information Technology Services department across the Gemini sites in Hawaii and Chile. A veteran IT professional, with over 25-years of experience in automotive and industrial computer manufacturing, pharmaceutical, and astronomy industries, he is an active, technical manager in services delivery, cybersecurity, and project management.

Tim holds certifications in IT security (Certified Information System Security Professional), project management (PRINCE2 Foundation) and virtualization (VMware Certified Professional). He attended Schoolcraft College, Washtenaw College, Eastern Michigan University, holds a degree in Digital Equipment Technology, and has studied business management & finance as well as mechanical engineering. Tim is currently immersed in the MSc Information Technology Management program at the University of Liverpool.

A long time supporter of the Akamai Workforce Initiative in Hawaii he actively participates with the program's selection committee and as a mentor. Tim is also a member of the University of Hawaii/Hawaii Community College Information Technology Program Advisory Committee, providing curriculum advisement.

Tim and his immediate family make their home in Hilo, Hawaii. In his spare time you might find (or hear) him spinning classic rock on vinyl at his home, or at the local racetrack, where, as the Regional Executive of the Big Island of Hawaii Sports Car Club of America, he and a team of dedicated supporters operate monthly race events.

*

Chris Morrison (CISSP) recently took the position of Information Technology Services department manager for the AURA/Gemini Observatory in Hilo, Hawaii and La Serena, Chile, and has been the Cyber Security liaison for the center for the past seven years. As an IT professional with 24 years experience, Chris has been involved in various aspects of information technology and Cyber Security within the scientific community including system design, identity management, risk assessment, awareness training, incident response, contract and project management. Prior to joining Gemini in 2006, Chris held positions at ESO's VLT project in Chile and the European Space Agency in Germany.

*

Anita Nikolich is Program Director for Cybersecurity in the Division of Advanced Cyberinfrastructure at the National Science Foundation (NSF). Prior to her work at the NSF she served as the Executive Director of Infrastructure at the University of Chicago. Past assignments include Director of Global Data Networking at Aon and Director of Security for Worldcom. She has explored how information technology and secure networking can best support the creation and sharing of scientific knowledge in virtual, mobile and physical contexts. She holds a Master of Science from The University of Pennsylvania and a Bachelor of Arts from the University of Chicago.

*

Irene Qualters is the Division Director of the Division of Advanced Cyberinfrastructure at NSF. As a recognized leader in cyberinfrastructure infrastructure, she represents NSF in several interagency and international efforts that span software, data, and computation. For example, she has represented NSF in the creation of the presidential initiative, NSCI.

Prior to her NSF career, Irene had a distinguished 30-year career in industry, with a number of executive leadership positions in the technology sector, in startups as well as a long tenure at Cray Research leading R&D, and six years with Merck Research Labs leading their Global Cyberinfrastructure for Research.

*

Susan Ramsey is a Risk Assessor and Security Engineer at the National Center for Atmospheric Research. She has over twenty years of experience building enterprise infrastructure and cloud computing. She joined NCAR in 2014 and promptly launched multiple initiatives to tackle compliance and identity management. Her latest projects include building a FISMA moderate segment and an organization wide Continuous Monitoring Plan. She has an MS in Computer Information Technology from Regis University, (thesis on Vulnerability Assessment). She is currently working towards a second Master of Science degree, in Information Security Engineering, from SANS Technical Institute.

*

Warren Raquel is a Senior Security Engineer at the National Center for Supercomputing Applications. His duties include security operations, incident response and security awareness for NCSA, Blue Waters and XSEDE. He has given talks and taught classes on Digital Forensics and Incident Response, two fields in which has specialized in for the last decade.

*

Scott Russell is the current Postdoctoral Fellow in Information Security Law & Policy at the Indiana University Center for Applied Cybersecurity Research. Scott's work has emphasized private sector cybersecurity best practices, data aggregation and the First and Fourth Amendments, and cybersecurity norms under international law. Scott studied Computer Science and History at the University of Virginia and received his J.D. from the Indiana University, Maurer School of Law.

*

Phil Salkie is a computer scientist who has been working as an industrial controls and automation engineer since 1984. His software and hardware designs serve sectors as diverse as food packaging, broadcast television, emergency power generation, water purification, sewage processing, surgical suture manufacture, biopharmaceuticals, specialty chemicals, laundry transport, semiconductor equipment manufacture, and nuclear power plant infrastructure. He is managing partner of Jeneriah, Industrial Automation.

*

Anurag Shankar is a senior security analyst at Indiana University's Center for Applied Cybersecurity Research (CACR). His expertise includes regulatory compliance (HIPAA and FISMA) and cybersecurity risk management. He has helped numerous institutions tackle HIPAA compliance and been

responsible for developing a NIST based risk management framework and using it to align IU's central research and enterprise cyberinfrastructures with HIPAA. His background also includes nearly twenty years with IU's central IT organization developing, delivering, and managing Unix support, massive data storage, the national Teragrid project, and supporting the research mission of the IU School of Medicine. He played a key role in building IU's research data storage environments, for supporting IU's Indiana Genomics Initiative and other life sciences efforts, and for creating information infrastructures and technology solutions for the Indiana Clinical and Translational Sciences Institute (CTSI). He is a computational astrophysicist by training (Ph.D. University of Illinois, '90).

*

Michael Sinatra has worked for the Energy Sciences Network (ESnet) since 2011, in the capacity of Network and Systems Engineer and Security Strategist. Prior to that, he worked for UC Berkeley for 19 years in both research and administrative positions. He has been interested in the nexus between system, security, and network for two decades. Sinatra holds degrees from Cornell and UC Berkeley.

*

Abe Singer works in the Security Group at the National Energy Research Supercomputer Center (NERSC) at Lawrence Berkeley Laboratory. Until recently, he was the the Chief Security Officer for the Laser Interferometer Gravitational Wave Observatory, operated by the California Institute of Technology. Prior to that he was the CSO of the San Diego Supercomputer Center at U.C. San Diego, and has had past lives as a private sector consultant, programmer, and system administrator.

*

Adam Slagell received an M.S. in computer science from the University of Illinois at Urbana-Campaign in 2003, a masters degree in mathematics from Northern Illinois University (NIU) in 2000, and a B.S. in mathematics from NIU in 1999. He currently serves as the director of the Cybersecurity Division and Chief Information Security Officer at the National Center for Supercomputing Applications (NCSA) where he co-leads the security team for the NSF-funded XSEDE federation, serves as liaison for the Bro Project at the Software Freedom Conservatory, and is a co-PI for the NSF Bro Center of Excellence, which brings its network security monitoring expertise and support to NSF-funded cyber-infrastructure and Higher Ed.

*

Susan Sons serves as a Senior Systems Analyst at Indiana University's Center for Applied Cybersecurity Research, having come from a background in abuse management, software development, and pentesting. In her free time, Susan volunteers as director of the Internet Civil Engineering Institute, a nonprofit dedicated to supporting and securing the common software infrastructure we all depend on, and as a search-and-rescue and disaster relief worker.

*

Amy Starzynski Coddens serves as the Education, Outreach and Training Manager at Indiana University's Center for Applied Cybersecurity Research (CACR). She is a graduate of the IU School of Education (M.S. '06 & M.S. '09). Amy comes to the CACR and CTSC from a background in P-16 education and outreach. She has worked for the government, in industry and in academia, contributing to projects with the New England Research Institute, Harvard's PEAR Institute, the United States Department of Education's Office of Special Education Programs, NASA and the IU Kelley School

of Business.

*

George Strawn had a short industrial career (4 years with IBM), a long academic career (30 years at Iowa State) and a pretty long government career (24 years at NSF). At Iowa State he served terms as chair of the Computer Science department and as director of the Computation Center. At NSF he invented the Internet (well, he was NSFnet program director and then division director of networking), then CISE executive officer and acting assistant director, and then served as CIO. He was detailed to OSTP in 2009 where he served as director of the NITRD NCO until his retirement in July of '15. But he failed retirement and has returned to work at NAS as board director for the Board on Research Data and Information. He has a PhD in mathematics from Iowa State and is a fellow of AAAS.

*

Patrick Storm is a Network Engineer with the Texas Advanced Computing Center at the University of Texas at Austin. Storm received his undergraduate degree from Oklahoma State University in Management Information Systems with an emphasis on Information Assurance. He joined the TACC team in March of 2013 and has spent most of his time there focusing on networking, operational security and incident response. Storm has been a part of the SCinet security team for the SC14, SC15, and SC16 Conferences, and is also a member of the XSEDE incident response and security teams.

*

Dr. Vicraj (Vic) Thomas is a Scientific Directory at BBN Technologies. He leads the Experimenter Support and Advocacy group within the GENI Project Office. The GENI Project Office provides the NSF with program management and systems engineering support in the design and development of GENI. Dr. Thomas' research interests include dependable systems and systems security. On the GENI project, Dr. Thomas was one of the systems engineers that developed a security plan for GENI. In the past he was a co-PI on an intrusion detector correlation project funded by the DARPA CyberPanel program and the PI of a project on the DARPA Cougaar program that developed intrusion detection agents.

*

Steve Tuecke co-leads the Globus project (www.globus.org) with Dr. Ian Foster, and is Deputy Director of the Computation Institute at The University of Chicago (UC) and Argonne National Laboratory. His focus is on the development of sustainable, cloud-based, software-as-a-service data management solutions to accelerate research. Prior to UC, Steven was co-founder, CEO and CTO of Univa Corporation from 2004-2008, providing open source and proprietary software for the high-performance computing and cloud computing markets. Before that, he spent 14 years at Argonne as research staff. Tuecke graduated with a B.A in mathematics and computer science from St. Olaf College.

*

Von Welch is the director of Indiana University's Center for Applied Cybersecurity Research (CACR) and PI for the NSF Cybersecurity Center of Excellence (CTSC). Additionally he is the CISO of the Software Assurance Market Place, a DHS-funded facility to foster software assurance and software assurance research, and serves on the InCommon Steering Committee as an advisor for the research community. Previously he has worked with a range of high-visibility projects to provide cybersecurity

to the broader scientific and engineering community, including TeraGrid, Open Science Grid, Ocean Observatory Infrastructure, and GENI. His work in software and standards includes authoring two IETF RFCS and the contributing to the creation of the well-known CILogon and MyProxy projects.

*

Dr. Carol Wilkinson is a visitor to NSF from the California Institute of Technology, providing support to the Large Facilities Office (LFO) on issues regarding the management of large scientific facilities. Her major roles while at NSF include being the LFO liaison to various facilities under construction, assisting with revisions of the Large Facilities Manual, and acting as the LFO liaison for Cyber Infrastructure. Her background includes research in experimental particle physics and experience in the operation and construction of large scientific facilities. She has formal training in facility and project management from the Project Management Institute (PMI) and other institutions. She earned certification in project management from the Stanford Advanced Project Management Institute.

Dr. Wilkinson gained familiarity with NSF construction projects funded through Major Research Equipment and Facility Construction (MREFC) accounts by serving for ten years as the project manager for the Advanced LIGO (Laser Interferometer Gravitational-Wave Observatory) development and construction. She also served on NSF construction project review panels for DUSEL, ALMA, OOI, NEON, and LSST. Previously, Dr. Wilkinson served as group leader and project manager for the construction and operation of two DOE funded accelerator facilities (DARHT) at Los Alamos National Laboratory before becoming project manager for the nuclear weapons testing program at DARHT before joining LIGO in 2003. She joined NSF on an Intergovernmental Personnel Act (IPA) assignment in November 2013.

*

Appendix C
Call for Participation

Call for Participation

2016 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

August 16 - 18 ✶ Westin Arlington Gateway ✶ Arlington, VA

http://trustedci.org/2016summit/

Theme: ***Strengthening Trustworthy Science***

It is our great pleasure to announce that the 2016 Summit will take place Tuesday, August 16th through Thursday, August 18th, at the Westin Arlington Gateway near the National Science Foundation Headquarters in Arlington, VA. On August 16th, the Summit will offer a full day of information security training tailored for the NSF community. The second and third days will follow a workshop format designed to increase the NSF community's understanding of cybersecurity strategies that strengthen trustworthy science: what data, processes, and systems are crucial to the scientific mission, what risks they face, and how to protect them.

About the Summit

Since 2004, the annual NSF Cybersecurity Summit has served as a valuable part of the process of securing the NSF scientific cyberinfrastructure by providing the community a forum for education, sharing experiences, building relationships, and establishing best practices.
The NSF cyberinfrastructure ecosystem presents an aggregate of complex cybersecurity needs (e.g., scientific data and instruments, unique computational and storage resources, complex collaborations) as compared to other organizations and sectors. This community has a unique opportunity to develop information security practices tailored to these needs, as well as break new ground on efficient, effective ways to protect information assets while supporting science. The Summit will bring together leaders in NSF cyberinfrastructure and cybersecurity to continue the processes initiated in 2013-2015: Building a trusting, collaborative community, and seriously addressing that community's core cybersecurity challenges.

The Summit seeks proposals for presentations, breakout and training sessions. It offers opportunities for student scholarships.

Proposing Content for the Summit

There are many ways to contribute to the Cybersecurity Summit. We are open to proposals for full- or half-day training sessions, for plenary presentations, and for breakout sessions. More specific information on each of those is available below. Submissions should be sent to CFP@trustedci.org by June 10th. Responses should go out by June 24th to ensure adequate planning time for presenters.

Proposing a Plenary Presentation

Please submit brief white papers focused on NSF Large Facilities' unmet cybersecurity challenges, lessons learned, and/or significant successes for presentation during the Summit Plenary Session (Aug 17-18). White papers (and presentations) may be in the form of position papers and/or narratives and may be one to five pages in length.

All submitted white papers will be included in the 2016 summit report. The Program Committee will select the most relevant, reasoned, and broadly interesting for presentation. A limited amount of funding is available to assist with travel for accepted submissions.

Submission deadline: June 10th
Submit to: CFP@trustedci.org
Word limit: 400 to 2000 words (~1-5 single spaced pages)
Notification of acceptance: June 24th

Proposing a Training Session

Training may be targeted at technical and/or management audiences, and be half-day or full-day in length. Areas of interest include, but are not limited to: cybersecurity planning and programs, risk assessment and management, regulatory compliance, identity and access management, data management and provenance, networks security and monitoring, secure coding and software assurance, physical security in the context of information security, and information security of scientific and emerging technologies. The Program Committee will select the most community-relevant and broadly interesting training sessions for presentation during the first day of the summit (Aug 16).

We generally prefer training sessions with some hands-on or interactive component over those that can be equally well presented in a non-interactive format (e.g. online videos), whether that component is a series of review Q&As, the opportunity to work directly with a piece of software or other tool, or a planning/management activity.

Submission deadline: June 10th
Submit to: CFP@trustedci.org
Word Limit: 600 words
Notification of Acceptance: June 24th

Proposing Table Top Sessions

In past years, the Summit has experimented with other formats for networking and information exchange, such as table-top topics at lunch. Proposals for such an activity should be 1-2 pages in length and include who would run the activity, the activity's intended audience, and a description of the activity itself and its expected benefits.

Submission deadline: June 10th
Submit to: CFP@trustedci.org
Word limit: 400 to 800 words (~1-2 single spaced pages)
Notification of acceptance: June 24th

Information for Students

Each year, the summit organizers invite several students to attend the summit. Reimbursement of travel expenses may be available. See http://trustedci.org/summit2016/students for more information.

Notes for First-Time Presenters

The Summit organizers want to encourage those who have not presented at previous Summits to share their experiences, expertise, and insights with the NSF cybersecurity community. You don't need to be perfectly polished, you just need to have something to share about your project or facility's experience with information security. Feedback from last year's Summit showed that there was a great deal of interest in "lessons learned" type presentations from projects who've faced cybersecurity challenges, and had to rethink some things afterwards. We've put together a page of tips and ideas for new presenters, including proposal and presentation tips as well as suggested topics. More direct coaching is available upon request.

Please contact CFP@trustedci.org with any questions, or to request help preparing a proposal or getting it ready to present at the Summit.

So you want to present at the 2016 NSF Cybersecurity Summit…

Welcome! The Summit organizers wish to encourage and support participation from throughout the wider NSF community. To further that mission, we've provided some information (below) to aid in the preparation of CFP responses. Please don't hesitate to direct questions to CFP@trustedci.org.

What to Present

This year's theme is "Strengthening Trustworthy Science." This is a subject that is the underlying motivation for all of the cybersecurity activities we pursue. The organizers especially appreciate proposals that drive this home, however, not every presentation, training session, or activity has to be centered around just that topic. Please submit any idea that you think may be relevant to our audience. If you would like to present, but aren't sure of what topic to choose, consider the following suggestions:

- **Lessons Learned**: *Get beyond the brag session. Tell the audience about something that DIDN'T go well for your project's cybersecurity efforts and how you overcame it. Even if you haven't overcome it yet, share the questions you are struggling with and open things up to the audience for Q&A or brainstorming. Too often, those doing cybersecurity in our community only see the big successes that others do press releases about, but there is even more to learn about the things that don't work.*
- Tools: *Have you discovered a new or unusual tool or technique that enables you in cybersecurity work? Do a "getting started" tutorial to help others learn about it so that they can implement it for themselves.*
- Enabling Cybersecurity Professional Development: *What do you do to find, train, and retain good people? How do you enable them to keep their skills fresh and growing?*
- *It would be great to get a session on approaches to building the cybersecurity workforce available to the science community.*

We strongly encourage proposals that address the 2015 Summit finding and recommendations:

- Security budget strategy / budget & program effectiveness
- Project leadership/stakeholders risk accountability and responsibility
- Software assurance

More details on the recommendations can be found in the 2015 NSF summit report: http://hdl.handle.net/2022/20539

Additionally, the following ideas might help you build a presentation idea around this year's theme, or work the theme into your presentation's topic:

- Supply chain requirements
- What are your most valuable and/or sensitive data?
    - What assets have you had the most trouble protecting?
    - Where have you found the best resources? For commodity technologies? For your special equipment?
- Have you gone through a process of formally identifying your information assets for security purposes? What does the documentation look like? What challenges have you faced (e.g., in classifying data)?

- Did you find anything assets that surprised you…. that you didn't think of as critical to the integrity of the scientific results?
- How do you assign responsibility for / stewardship of specific information assets (or sets of assets that serve a process) within your organization? When if ever does security have direct accountability for the security of these assets?

How to Build a CFP Response

The proposal you submit will be used in two ways: to tell the organizers about what you plan to present, and to be included in the summit findings as a sort of after-action report. It should include:

- An executive summary (short description of the topic and content).
- Who the presenter(s) is/are.
- Either a whitepaper discussion of the topic, or a narrative you'd like to share with the community. (For activities that are not trainings or plenary sessions, this may be replaced with a description of the planned activity, any space or equipment needs, and the activity's intended audience.)
- Contact information (preferably email) for the presenter(s) in case the organizers have any questions. This can be in a separate note in the email body instead of the proposal itself if presenter(s) don't wish it to be published.
- Expected length of the session/training/activity. Generally, trainings are either full- or half-day and plenary sessions are about 50 minutes, but if a good idea takes more time than that, we will work with presenters to make it happen.
- Any relevant references (e.g. link to the home page for the project the talk is about, or recommendations for further reading).

Our community has expressed in the past that many find it helpful if they can download a copy of a presentation's slides. If you are willing to publish your slides, please email a copy (or a link to where you prefer to host slides) to CFP@trustedci.org.

The easiest way to get help/feedback from the organizing committee prior to submitting your final proposal is to create a Google Doc containing your proposal and sending an edit link to CFP@trustedci.org. Don't share directly with that address, as the link will be passed on to a reviewer who will have their own google account.

Tips for Presenting

There are many different presentation formats that can work well, depending on the topic. Consider the following:

Lecture format : The presenter(s) talk to the audience and show slides to support their dialogue, then do a short Q&A time at the end of the presentation.

Panel format: 3-5 persons answer questions offered by a moderator on a specific topic or set of topics, then do a short Q&A with the audience. This tends to work out best when the panel contains people with very different backgrounds or viewpoints, and the moderator is good at keeping folks to the topic and time constraints.

Open Forum format: 2-3 persons answer questions offered by the audience. Works best if there is an extra person gathering questions and presenting them, and if the speakers can keep things succinct so that the presentation keeps moving and many questions get answered.

Hands-on format: The presenter(s) walk the audience through a demo or tutorial as the audience follows along on their computers (or on paper, if the topic supports it). If you are doing a training that will have many hands-on activities, consider having more than one presenter, or a presenter plus a helper or two who can go around the room and help participants who get stuck, allowing the group as a whole to move on.

Whatever format you choose, be sure to engage your audience by making eye contact (with them, not with the slide screen!), showing interest in what you are saying, and not rushing. Most speakers appear most smooth and practiced when following a general outline they've practiced once or twice, rather than trying to read a prepared script verbatim.

Appendix D
Training Descriptions

Training Sessions *August 16* 2016 NSF Cybersecurity Summit

Tuesday, August 16 will feature a full day of training, available to all registrants. All but the *Log Analysis Training with CTSC and Bro* and *Federated Identity Management for Research Organizations* are half-day offerings. Seating may fill for some or all sessions, and pre-event registration for individual sessions is required to reserve a seat. Please register by August 11 to guarantee seating and help us make final preparations. Direct inquiries to Amy Starzynski Coddens (astarzyn@indiana.edu).

Concurrent Morning Sessions

Log Analysis Training with CTSC and Bro (Full Day)

Instructors: Vlad Grigorescu, Warren Raquel, Adam Slagell, Jeannette Dopheide (NCSA)

CTSC is partnering with members of the Bro Project to present a full-day training on log analysis for operations security, providing a detailed walkthrough of the log analysis life cycle with interactive demonstrations using the Bro network analysis software. The training will be applicable to those just starting or those expanding their security logging and monitoring infrastructure. No prior experience with Bro is required. The training will teach lessons that can be generalized to other kinds of system and network logs, whether or not a site is using or plans to use the Bro software.

The goal of security log analysis is to more efficiently leverage log collection in order to identify threats and anomalies in their cyberinfrastructure. This training will help attendees tie various log and data sources together to provide a more rounded, coherent picture of a potential security event. It will also help attendees understand log analysis as a life cycle that continues to become more efficient over time.

The training will cover the four phases of the log analysis life cycle: Monitoring, Event Management, Analysis, and Response. It will demonstrate how proper management of these four phases contributes to a security team's effectiveness. Interactive demonstrations will cover both automated and manual analysis using multiple log sources (network protocols, files, software, intel, etc.), with examples from real security incidents. Lastly, the training will cover how to use lessons learned during each cycle to tune the monitoring and analysis workflow to improve an organization's operational security footing over time.

Federated Identity Management for Research Organizations (Full Day)

Instructors: Jim Basney (NCSA and University of Illinois / CTSC) and Scott Koranda (Spherical Cow Group / CTSC)

Research Organizations and Collaborations, and especially virtual organizations (VOs), come together to solve complex problems leveraging people and resources from multiple institutions, often spanning the world. Expert in their respective domains, VOs rarely have expertise in the identity management aspects of collaboration. Regardless of VO size, properly designed identity management processes and technologies can help facilitate VO research by providing access to collaboration tools and services quickly, and removing that access when it should no longer be granted.

This full-day tutorial will provide an overview of the issues in identity management facing and solutions available to VOs, in order to help them more easily manage access to their resources.

Topics covered will include:

- Understanding the identity management process needs of VOs of any size
- Leveraging Federated and Social Identity to authenticate VO participants

- Understanding the complexities of international federation and collaboration
- Passwords, Certificates, SSH Keys, and other authentication technologies: what works where?
- Participant lifecycle management using open source identity management solutions, including COmanage, Grouper, and Shibboleth
- Application Integration and Provisioning, from the shell to the web to the cloud: how to make apps work with identity management infrastructure

Interactive demonstrations will be used to provide tangible insight into the capabilities of various solutions.

REN-ISAC Cyberthreat Training (30 Minute Introduction to Developing Cybersecurity Programs for NSF Projects)

Instructors: Kim Milford and Todd Herring (REN-ISAC)

Cyber-attacks can be extremely damaging for research organizations. Damages - and costs - include stolen funds, damaged systems, the cost of time while out of service or time to recover, regulatory fines, legal damages, financial compensation for injured parties, loss of business partner trust, and loss of integrity due to compromised digital assets. Being resilient to cyber-risks starts with knowing about the risks to research and academic organizations:

- What are the biggest threats?
- What assets are at greatest risk?
- What are the tactics, techniques and practices (TTPs) used by your adversaries?
- What are the possible scenarios for attack? and
- What is the potential impact to your research?

Insight into cyber-threats allows organizations to develop appropriate risk management and reduce risk exposure through well-balanced cyber-defense Although it's never possible for any organization to be 100% secure, it is entirely possible to use a mix of processes for prevention, detection, and response to keep cyber-risk below an appropriate level and enable an organization to operate with less disruption.

Developing Cybersecurity Programs for NSF Projects

Instructors: Bob Cowles, Craig Jackson, Jim Marsteller, Susan Sons (CTSC)

This instructional session will be based on a cybersecurity planning guide (see trustedci.org/guide) developed with input from the Daniel K. Inouye Solar Telescope (DKIST) project, and in use at a number of NSF facilities and projects. The Guide was developed to address the information security requirements outlined in NSF cooperative agreements, and provide solid guidance, tools, and resources. This session will be appropriate both for attendees of last year's training of the same name, as well as newcomers. Though there will be a good deal of overlap, we will be updating our presentation, and supporting opportunities to explore areas in greater depth based on participants' needs. Some of the topics that will be covered include:

- Building or Improving an Information Security Program
- Unique and Critical Science Requirements, Constraints, and Security Controls
- Information Security Policies and Procedures
- The Role of Project Leadership and Risk Acceptance
- Establishing a Risk Management Approach to Information Security
- Defining, Identifying, and Classifying Information Assets
- The Role of Risk Assessments within the Program Lifecycle
- Baseline Controls and Best Practices
- Topical Information Security Considerations: Third-Party Relationships, Asset Management, Access Control, Physical Security, Monitoring, Logging, and Retention

- Program Assessment and Evaluation

While this session will be instructional in nature, it is also intended to be an interactive session to seek constructive feedback from attendees to further improve the guide. There will be significant opportunities for discussion and Q&A.

Building a NIST Risk Management Framework for HIPAA and FISMA Compliance

Instructor: Anurag Shankar (Indiana University)

Every federal agency and its subcontractors are required by law to comply with the Federal Information Security Management Act (FISMA). With cyberattacks and cybercrime now an increasingly integral and permanent part of the cyber landscape, funding agencies are beginning to require FISMA compliance from their R&D subcontractors such as large facilities. In other cases, protected health information (PHI) subject to the federal Health Insurance Portability and Accountability Act (HIPAA) is beginning to leak into organizations that handle for instance emerging areas such as genomics, big data and analytics. In both cases, the most formidable challenge when facing regulatory compliance for the first time is a complete lack of bearing. Often, peers cannot be easily found and a lonely and steep learning curve must be scaled. A common reaction in such cases is to reply on technical controls alone such as firewalls, etc. with the mistaken assumption that they will keep the bad actors out. Not carefully considering the effectiveness of controls in mitigating risk results in both inadequate security as well as misdirected effort.

FISMA requires the adoption of cybersecurity guidelines developed by the National Institute of Standards and Technology (NIST). NIST provides a comprehensive and flexible risk management framework that can be customized to fit any organization or environment, irrespective of FISMA. NIST also provides an all-inclusive catalog of practically every conceivable security control to choose from. The NIST guidelines are also considered as a cybersecurity standard today and adopted by a wide variety of organization within and outside the government. They allow one to comply not only with FISMA but with other rules and regulations such as HIPAA. This workshop will familiarize the participant with both HIPAA and FISMA and provide guidance on how to build and deploy a NIST based risk management framework to both handle compliance and to gain a deeper understanding of cybersecurity and how to manage it.

Topics Covered:

- HIPAA and FISMA Regulations: An introduction to the regulations, common misperceptions, where and how they apply.
- The NIST Risk Management Framework. A dive into risk management and security controls covered by NIST special publications 800-30 and 800-53.
- Building Your Own Risk Management Framework. Scoping, planning, controls, initial risk assessment, risk mitigation, documentation, ongoing risk management, reviews and training.

Secure Coding Practices and Automated Assessment Tools

Instructors: Prof. Barton P. Miller and Prof. Elisa Heymann (University of Wisconsin / CTSC)

This tutorial is relevant to anyone wanting to learn about minimizing security flaws in the software they develop or manage. We share our experiences gained from performing vulnerability assessments of critical middleware. You will learn skills critical for software developers and analysts concerned with security.

Software assurance tools - tools that scan the source or binary code of a program to find weaknesses - are the first line of defense in assessing the security of a software project. These tools can catch flaws in a program that can affect both the correctness and safety of the code. This tutorial is also relevant to anyone wanting to learn how to use these automated assessment tools to minimize security flaws in the software they develop or manage.

This tutorial starts by presenting basic concepts related to threats, weaknesses and vulnerabilities. We will also show how to think like an attacker. Then we will present coding practices that lead to vulnerabilities, with examples of how they commonly arise, techniques to prevent them, and exercises to reinforce your skills in avoiding them. Examples come from a wide variety of languages, including Java, C, C++, C#, Perl, Pythos, and Ruby, and come from real code belonging to Cloud and Grid systems we have assessed. The new addition to the tutorial covers software assurance tools work, so that the student can understand the capabilities and limitations of such tools. We then focus on a selection of both commercial and open source tools for C/C++ and Java, and demonstrate how to apply them to sample programs with known flaws.

Concurrent Afternoon Sessions

Log Analysis Training with CTSC and Bro (continued)

See full description above.

Federated Identity Management for Research Organizations (continued)

See full description above.

Securing Legacy Industrial Control Systems

Instructor: Phil Salkie (Jenariah Industrial Automation)

Scientific and technical facilities worldwide incorporate Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) systems into their mix of technologies - often without the knowledge or support of the on-side IT department. These systems can include decades-old designs, contain firmware which is not (or cannot) be updated or patched, and can have long lists of known vulnerabilities - yet they continue to be placed into network environments throughout the world. This breakout session will explore a range of devices and techniques which are available to IT departments and network engineers to isolate, monitor, and protect these often mission-critical Industrial Control System (ICS) networks without replacing older devices nor obtaining access from vendors to proprietary controller software.

Building the Modern Research Data Portal Using the Globus Platform

Instructor: Steve Tuecke (University of Chicago)

New Globus REST APIs, combined with high-speed networks and Science DMZs, create a research data platform on which developers can create entirely new classes of scientific applications, portals, and gateways. Globus is an established service that is widely used for managing research data on XSEDE, DOE, and campus computing resources, and it continues to evolve with the addition of data publication capabilities, and enhancement of the core data transfer and sharing functions. Over the past year we have added new identity and access management functionality that will simplify access to Globus using campus logins, and facilitate the integration of Globus, XSEDE, and other research cyberinfrastructure services into web and mobile applications can leverage Globus and Science DMZs to provide a broad range of researchers with access to advanced data management capabilities using existing organizational credentials. A combination of presentation and hands-on exercises will result in attendees learning how to build and run a simple, yet fully functional, web application that can be leveraged their own applications.

Secure Software Engineering Best Practices

Instructors: Randy Heiland and Susan Sons (CTSC)

This interactive training session will introduce participants to a broad range of tools and methodologies for promoting secure software development throughout the software life cycle. Learn how software repositories, testing, static analysis, vulnerability management process, release/delivery management methods, integrated development environments (IDEs), and documentation can enhance or impair the security of the software that is written and released by any team. Participants are encouraged to follow along on their laptops for the most hands-on experience, but this is not required.

Appendix E
Listing of Attendees and Organizations

Your Name	Your Organization / Institution
Abe Singer	NERSC, Lawrence Berkeley Laboratory
Adam Slagell	NCSA
Alexander Withers	NCSA
Amy Starzynski Coddens	CACR/Indiana University
Amy Walton	Advanced Cyberinfrastructure Division, National Science Foundation
Andrew Ferbert	San Diego Supercomputer Center
Andrew Gallo	The George Washington University
Andrew K Adams	CTSC
Anita Nikolich	NSF
Anthony Skjellum	Auburn University
Anurag Shankar	Indiana University
Ardoth Hassler	Georgetown University
Aunshul Rege	Temple University
Barb Fossum	BMF Consulting
Barton Miller	University of Wisconsin-Madison
Bill Miller	National Science Foundation
Bob Cowles	CTSC / BtightLite Info Sec
Bob Houtman	NSF
Bret Goodrich	National Solar Observatory
Brian Markham	The George Washington University
Cesar Flores	IODP, TAMU
Chris Morrison	Gemini Observatory
Christopher Thompson	Purdue University
Cliff Jacobs	Clifford A. Jacobs Consulting LLC
Craig Jackson	CTSC / Indiana University CACR
Dave Dykstra	Fermilab
David Goodwin	U.S. Dept of Energy
David Halstead	National Radio Astronomy Observatory
Deja T. Jackon	Kennesaw State University
Diana Borecky	CACR
Diane Murphy	Marymount University
Dominique Dalanni	California State University, Dominguez Hills

Your Name	Your Organization / Institution
Don DuRousseau	George Washington University
Doug Pearson	REN-ISAC
Elisa Heymann	University of Wisconsin-Madison
George Strawn	National Academy of Sciences, Engineering and Medicine
Irene Qualters	NSF
James Babcock Hughes	Cerro Tololo Interamerican Observatory
James Marsteller	Pittsburgh Supercomputing Center
Jamie Allan	National Science Foundation
Jeannette Dopheide	CTSC
Jeff Leithead	NSF
Jim Basney	NCSA
Jim Rosser	Texas A&M University
Joy Pauschke	National Science Foundation ENG/CMMI
JUAN F. Arratia	Ana G. Mendez University System, San Juan, Puerto Rico
Justin Platt	Northern Virginia Community College
Justin R. Davis	University of Florida
Keith Hartranft	Lehigh University
Kevin Thompson	NSF
Kimberly Milford	REN-ISAC
Larry Wallace	Caltech
Leslee Cooper	CACR
Mark Coles	National Science Foundation
Mark Krenz	CTSC / CACR
Mark Patton	University of Arizona - Management Information Systems
Michael Corn	Brandeis University
Michael Sinatra	Energy Sciences Network
Miron Livny	University of Wisconsin-Madison
Nathaniel Mendoza	TACC/UT
Nikita Golubets	Eastern Michigan University
Nino Simonishvili	National Cybersecurity Institute at Excelsior College
Noor Aarohi	The George Washington University
Patricia Okorie	Prince George's Community College

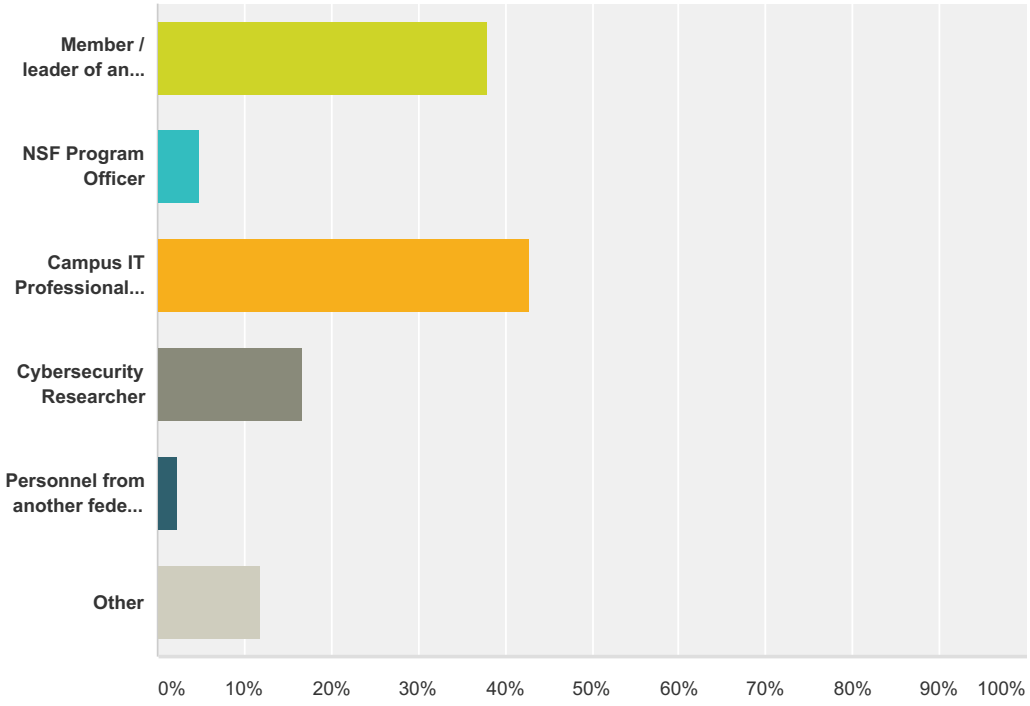
Your Name	Your Organization / Institution
Patrick Murphy	National Radio Astronomy Observatory
Patrick Storm	Texas Advanced Computing Center
Peter Jensen	Florida State University
Peter Kuper	In-Q-Tel
Phil Salkie	Jenariah Industrial Automation
Purushotham Bangalore	University of Alabama at Birmingham (UAB)
Ragib Hasan	University of Alabama at Birmingham
Randy Heiland	CACR/Indiana University
Raphael Greenbaum	Wall of Wind, Florida International University
Rasib Khan	University of Alabama at Birmingham
Robert Kent	NHERI UTexas
Rod Rutland	National Optical Astronomy Observatory
RuthAnne Bevier	Caltech
Ryan Kiser	Indiana University CACR
Ryan L. Richmond	AURA
Scott Koranda	Center for Trustworthy Scientific Cyberinfrastructure
Shannon Roddy	Penn State
Shijie Yang	The Cornell High Energy Synchrotron Source / Cornell University
Steve Barnet	UW-Madison
Steve Cleveland	Oregon State University
Steve Tuecke	Globus / UChicago / Argonne
Steven Geiger	National Radio Astronomy Observatory
Susan Ramsey	NCAR - National Center for Atmospheric Research
Susan Sons	CACR, Indiana University
Taína Muñoz-Mulero	National Science Foundation
Terry Fleury	Univ. of Illinois / NCSA
Tim Howard	National Science Foundation
Tim Minick	HPM
Tony Baylis	Lawrence Livermore National Laboratory
Vic Thomas	BBN Technologies
Victor Hazlewood	University of Tennessee
Vitaly Ford	Tennessee Tech University

Your Name	Your Organization / Institution
Vlad Grigorescu	NCSA
Von Welch	CACR / Indiana University
Warren Raquel	CTSC

Appendix F
Attendee Survey summary report

Q1 Which options best describe your job or position? Check all that apply.

Answered: 42 Skipped: 0



Answer Choices	Responses	
Member / leader of an NSF project	**38.10%**	16
NSF Program Officer	**4.76%**	2
Campus IT Professional / CIO	**42.86%**	18
Cybersecurity Researcher	**16.67%**	7
Personnel from another federal program (NSA, DOE/ESNet, etc.)	**2.38%**	1
Other	**11.90%**	5
Total Respondents: 42		

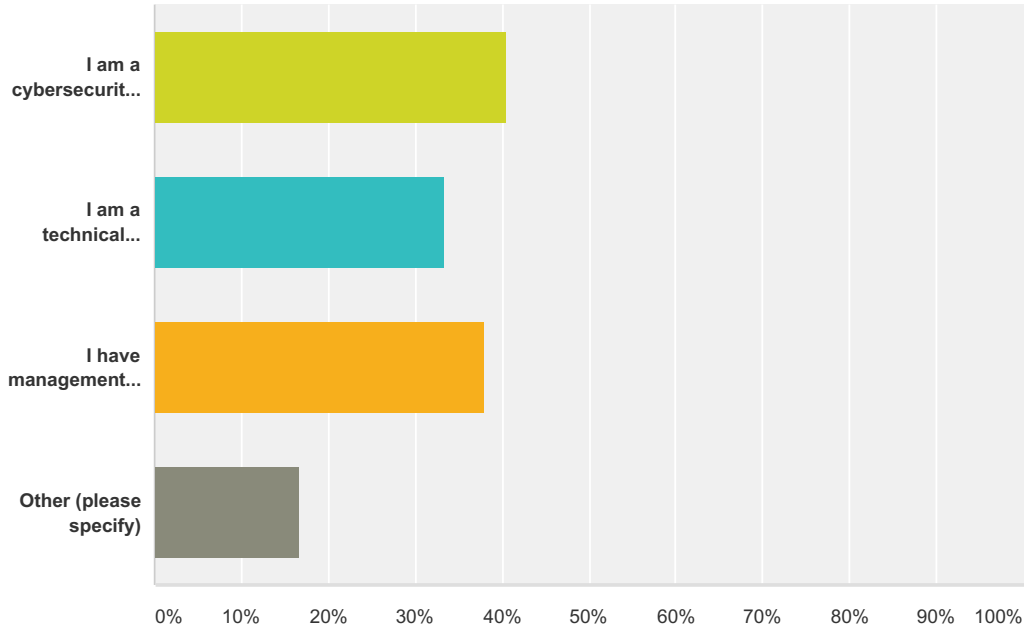
Q2 Where do you work primarily?

Answered: 42 Skipped: 0

Answer Choices	Responses	
State/Province:	**97.62%**	41
Country:	**97.62%**	41

Q3 How would you characterize your job in relationship to cybersecurity? Please check all that apply.

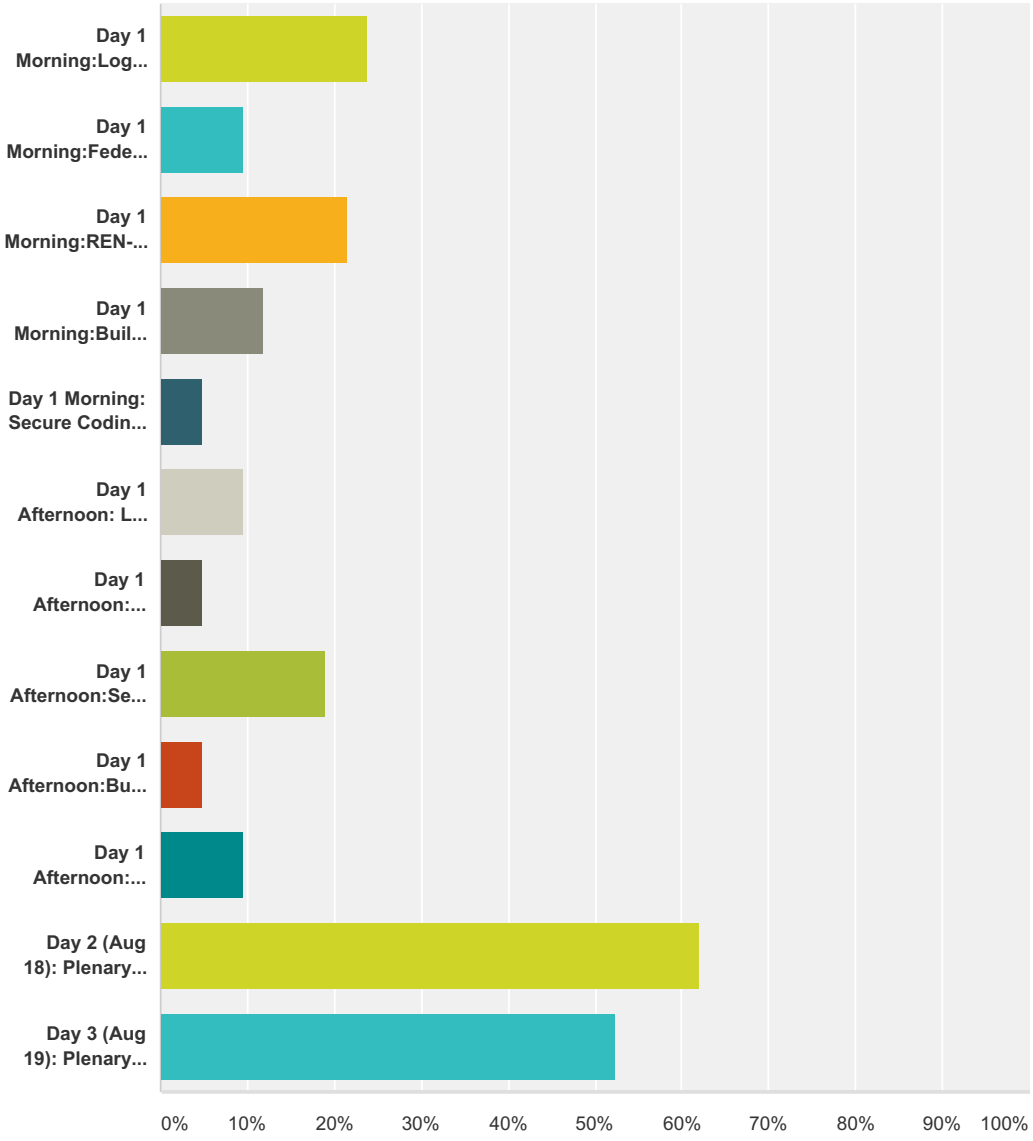
Answered: 42 Skipped: 0



Answer Choices	Responses	
I am a cybersecurity professional	**40.48%**	17
I am a technical professional who has knowledge of cybersecurity	**33.33%**	14
I have management responsibility for cybersecurity	**38.10%**	16
Other (please specify)	**16.67%**	7
Total Respondents: 42		

Q4 What sessions of the summit did you attend? Check all that apply.

Answered: 42 Skipped: 0

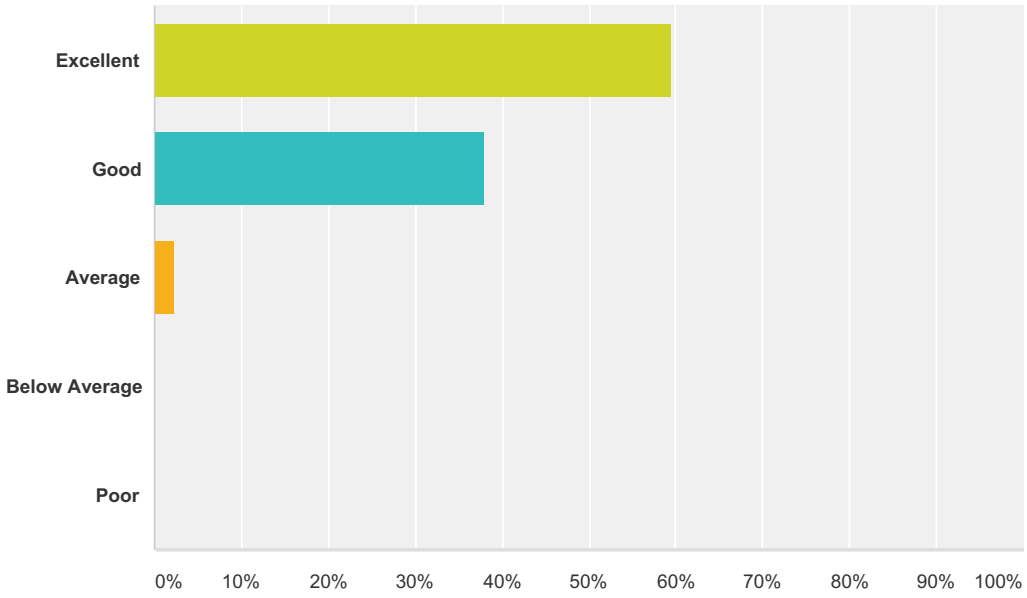


Answer Choices	Responses	
Day 1 Morning:Log Analysis Training with CTSC and Bro	23.81%	10
Day 1 Morning:Federated Identity Management for Research Organizations	9.52%	4
Day 1 Morning:REN-ISAC Cyberthreat Training / Developing Cybersecurity Programs for NSF Projects	21.43%	9
Day 1 Morning:Building a NIST Risk Management Framework for HIPAA and FISMA Compliance	11.90%	5
Day 1 Morning: Secure Coding Practices and Automated Assessment Tools	4.76%	2
Day 1 Afternoon: Log Analysis Training with CTSC and Bro(continued)	9.52%	4
Day 1 Afternoon: Federated Identity Management for Research Organizations(continued)	4.76%	2

Day 1 Afternoon:Securing Legacy Industrial Control Systems	**19.05%**	8
Day 1 Afternoon:Building the Modern Research Data Portal Using the Globus Platform	**4.76%**	2
Day 1 Afternoon: Secure Software Engineering Best Practices	**9.52%**	4
Day 2 (Aug 18): Plenary Session	**61.90%**	26
Day 3 (Aug 19): Plenary Session	**52.38%**	22
Total Respondents: 42		

Q5 How would you rate your overall experience with the 2016 summit?

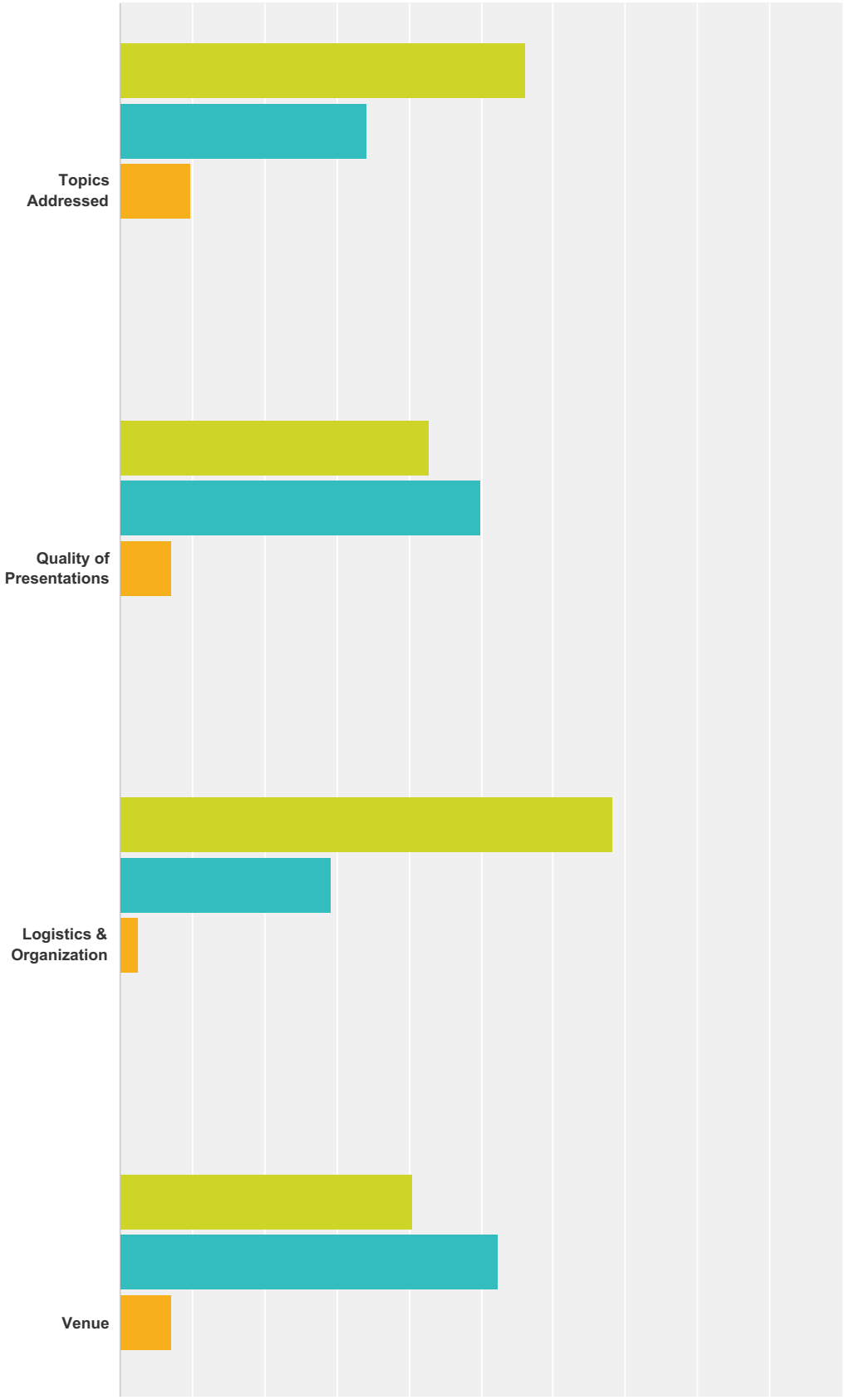
Answered: 42 Skipped: 0

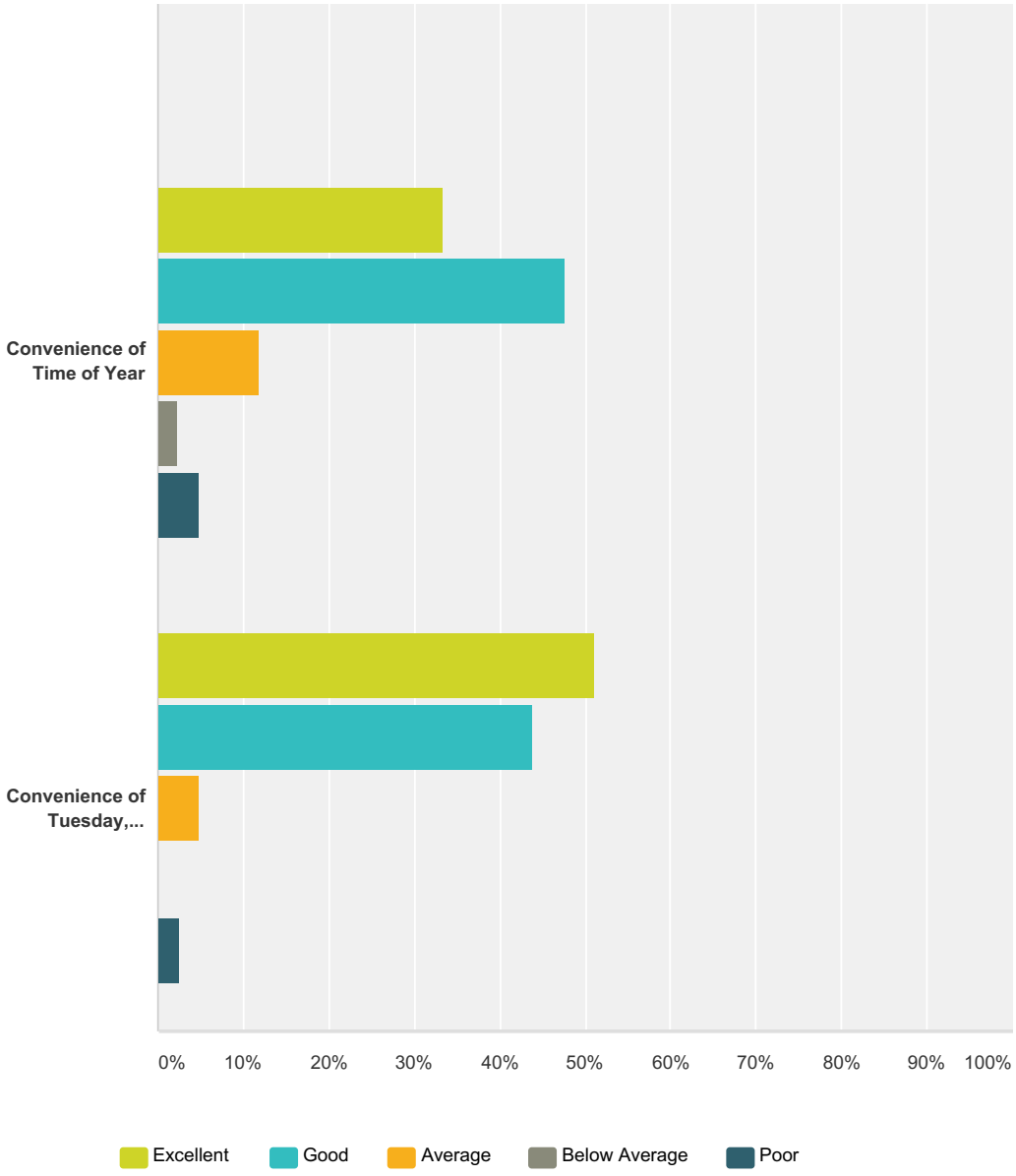


Answer Choices	Responses	
Excellent	**59.52%**	25
Good	**38.10%**	16
Average	**2.38%**	1
Below Average	**0.00%**	0
Poor	**0.00%**	0
Total		**42**

Q6 Please rate your experience with the 2016 summit in these areas:

Answered: 42 Skipped: 0

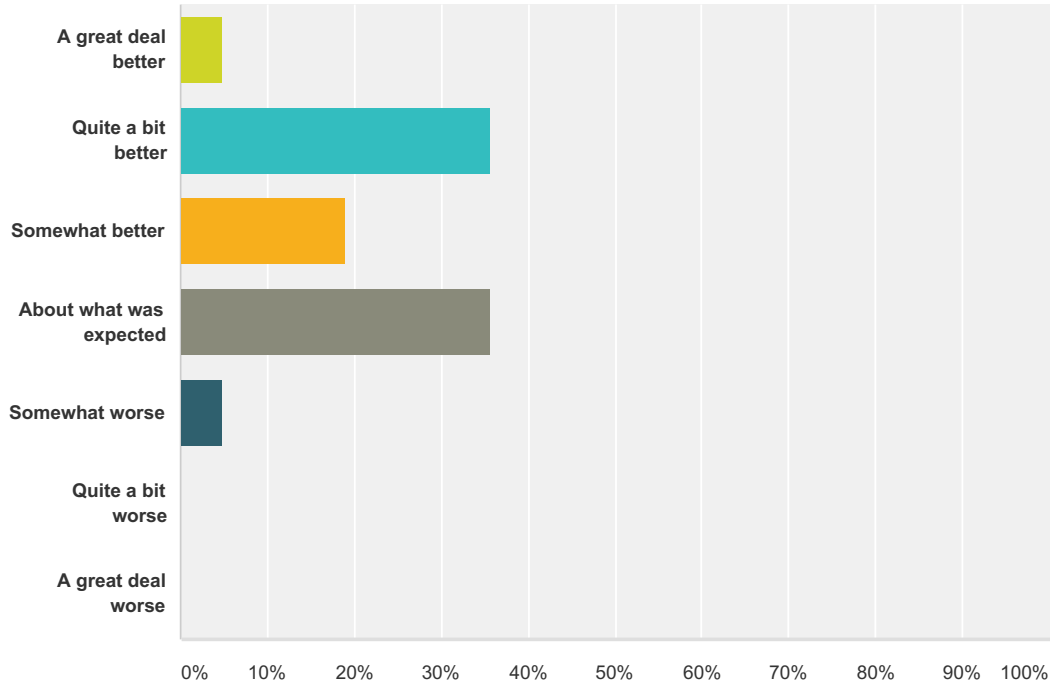




	Excellent	Good	Average	Below Average	Poor	Total Respondents
Topics Addressed	**56.10%** 23	**34.15%** 14	**9.76%** 4	**0.00%** 0	**0.00%** 0	41
Quality of Presentations	**42.86%** 18	**50.00%** 21	**7.14%** 3	**0.00%** 0	**0.00%** 0	42
Logistics & Organization	**68.29%** 28	**29.27%** 12	**2.44%** 1	**0.00%** 0	**0.00%** 0	41
Venue	**40.48%** 17	**52.38%** 22	**7.14%** 3	**0.00%** 0	**0.00%** 0	42
Convenience of Time of Year	**33.33%** 14	**47.62%** 20	**11.90%** 5	**2.38%** 1	**4.76%** 2	42
Convenience of Tuesday, Wednesday, Thursday Dates	**51.22%** 21	**43.90%** 18	**4.88%** 2	**0.00%** 0	**2.44%** 1	41

Q7 Was this summit better than what you expected, worse than what you expected, or about what you expected?

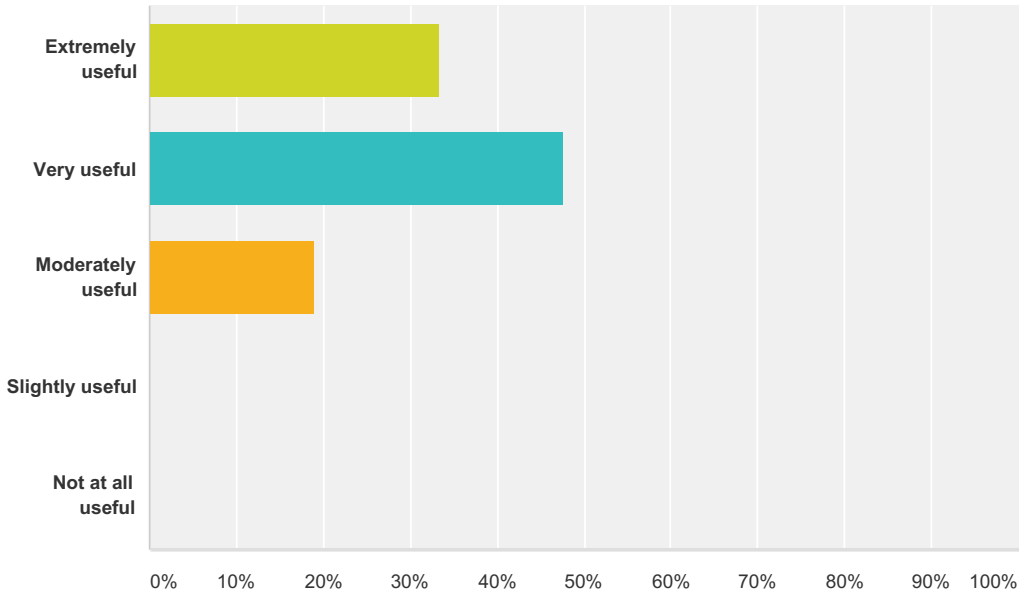
Answered: 42 Skipped: 0



Answer Choices	Responses	
A great deal better	**4.76%**	2
Quite a bit better	**35.71%**	15
Somewhat better	**19.05%**	8
About what was expected	**35.71%**	15
Somewhat worse	**4.76%**	2
Quite a bit worse	**0.00%**	0
A great deal worse	**0.00%**	0
Total		**42**

Q8 How useful to your work was the information discussed at the summit?

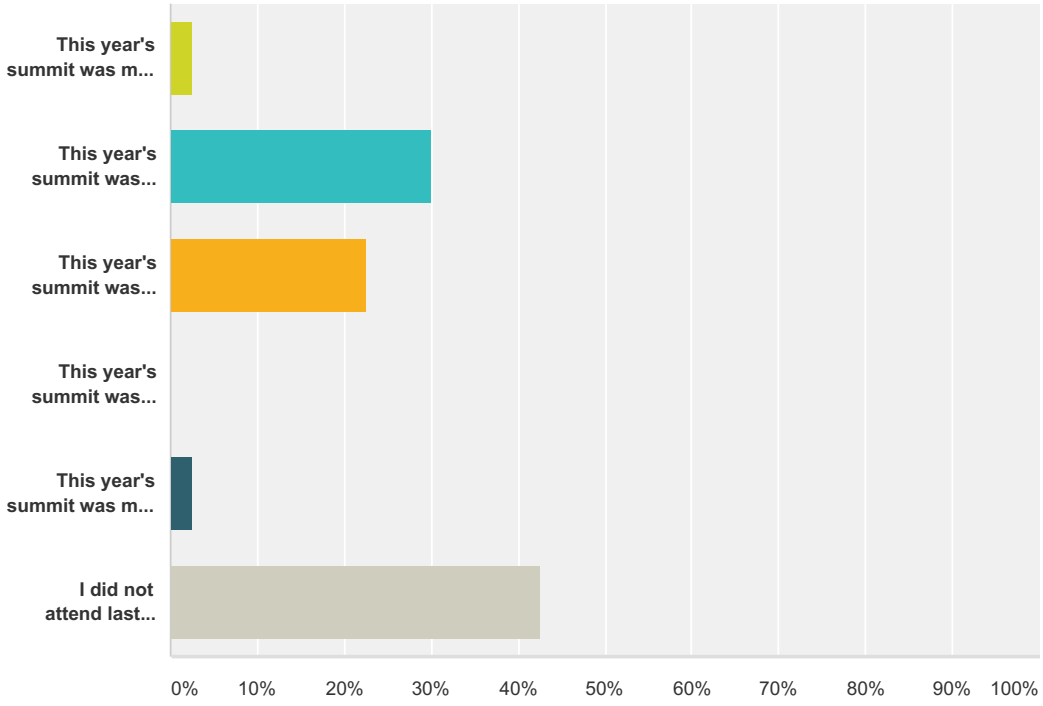
Answered: 42 Skipped: 0



Answer Choices	Responses	
Extremely useful	**33.33%**	14
Very useful	**47.62%**	20
Moderately useful	**19.05%**	8
Slightly useful	**0.00%**	0
Not at all useful	**0.00%**	0
Total		**42**

Q9 If you attended last year's summit, how does this year's compare?

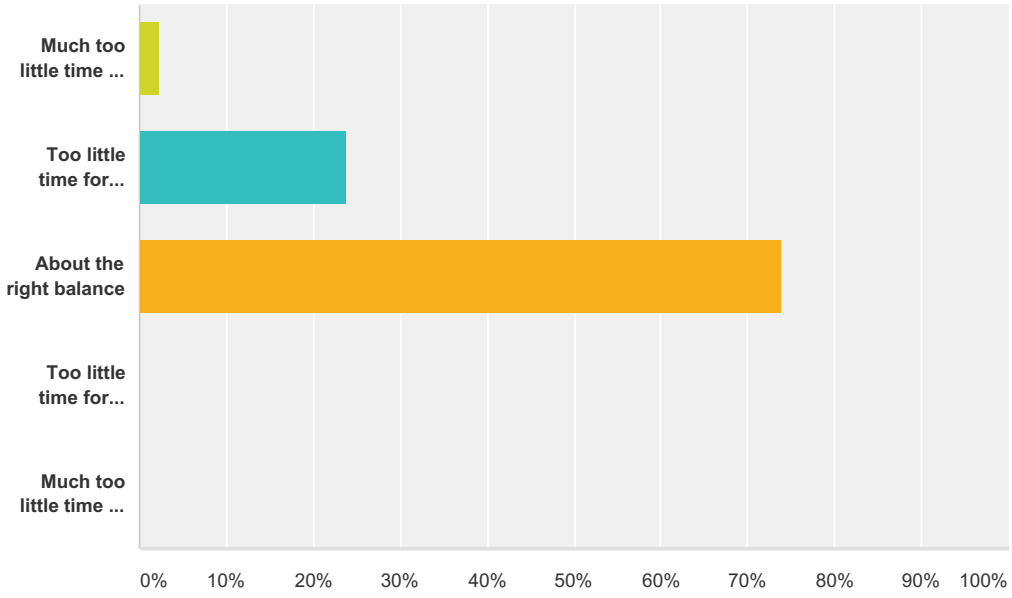
Answered: 40 Skipped: 2



Answer Choices	Responses	
This year's summit was much better than last year's.	2.50%	1
This year's summit was better than last year's.	30.00%	12
This year's summit was about the same as last year's.	22.50%	9
This year's summit was worse than last year's.	0.00%	0
This year's summit was much worse than last year's.	2.50%	1
I did not attend last year's summit.	42.50%	17
Total		**40**

Q10 How would you describe the balance between structured presentations and informal networking opportunities?

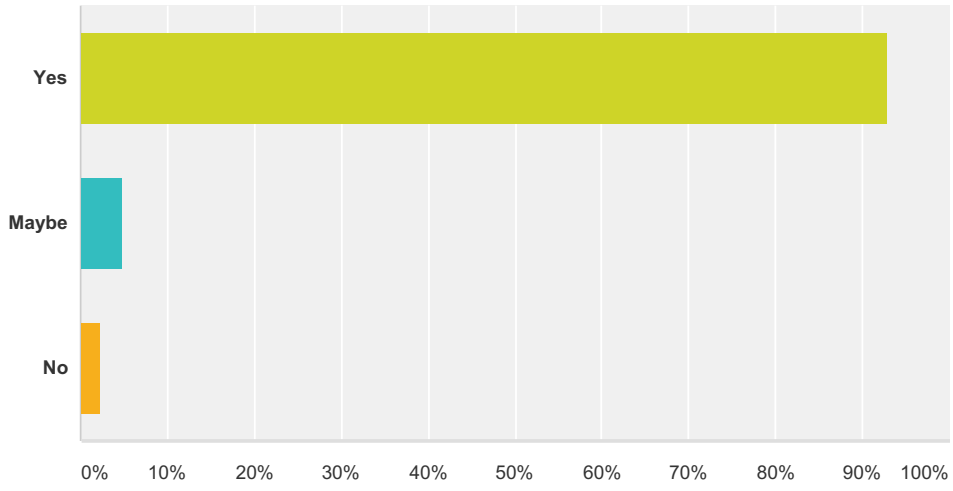
Answered: 42 Skipped: 0



Answer Choices	Responses	
Much too little time for informal networking	**2.38%**	1
Too little time for informal networking	**23.81%**	10
About the right balance	**73.81%**	31
Too little time for structured presentations	**0.00%**	0
Much too little time for structured presentations	**0.00%**	0
Total		**42**

Q11 Would you like to attend future summits?

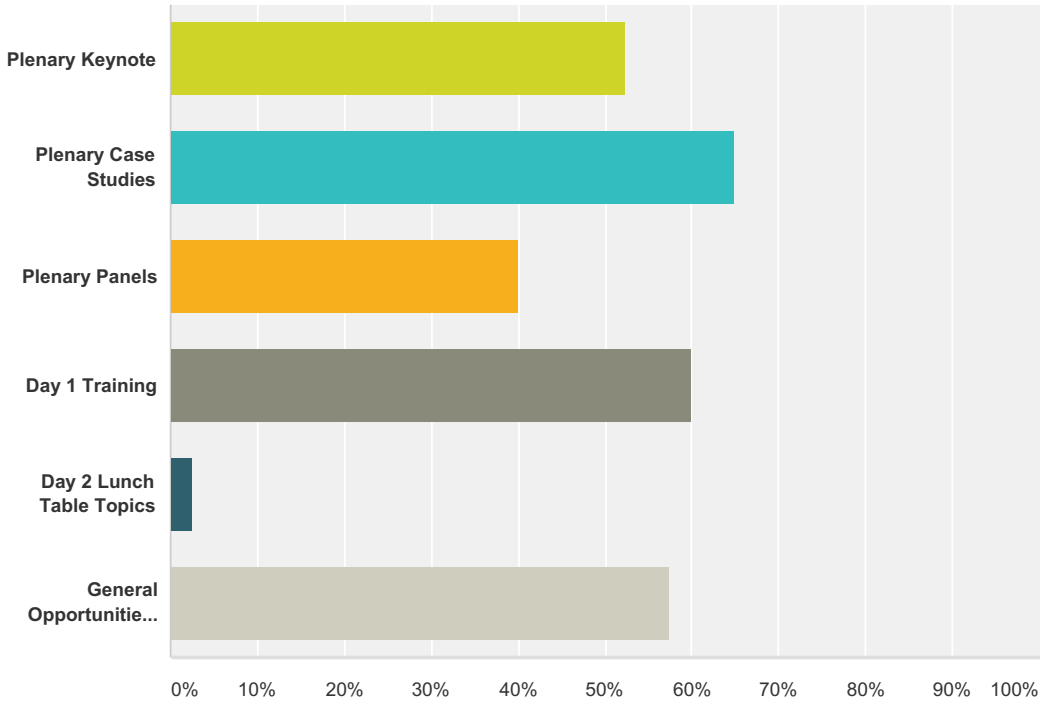
Answered: 42 Skipped: 0



Answer Choices	Responses	
Yes	**92.86%**	39
Maybe	**4.76%**	2
No	**2.38%**	1
Total		**42**

Q12 What presentation format(s) did you find most valuable? (You may select more than one.)

Answered: 40 Skipped: 2

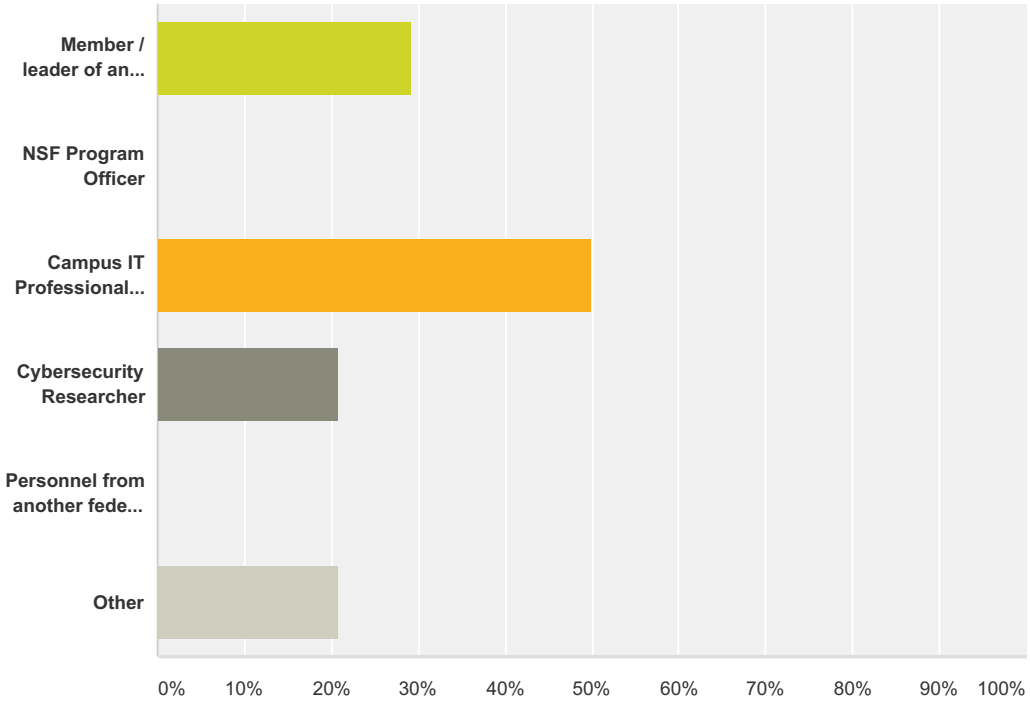


Answer Choices	Responses	
Plenary Keynote	**52.50%**	21
Plenary Case Studies	**65.00%**	26
Plenary Panels	**40.00%**	16
Day 1 Training	**60.00%**	24
Day 2 Lunch Table Topics	**2.50%**	1
General Opportunities to Network	**57.50%**	23
Total Respondents: 40		

Appendix G
Training Evaluation Survey Summary Report

Q1 Which options best describe your job or position? Check all that apply.

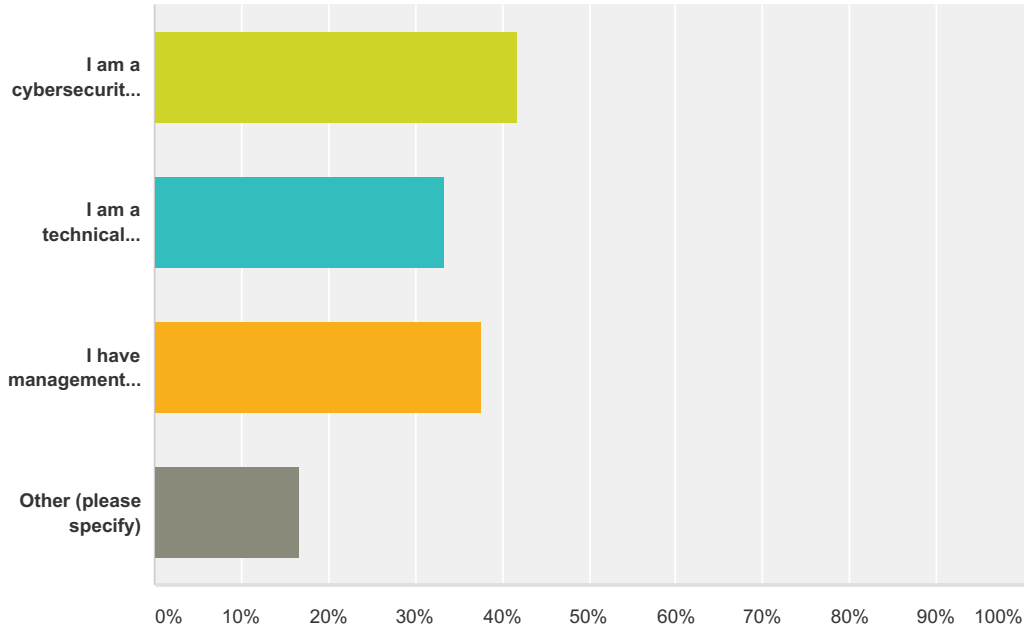
Answered: 24 Skipped: 0



Answer Choices	Responses	
Member / leader of an NSF project	**29.17%**	7
NSF Program Officer	**0.00%**	0
Campus IT Professional / CIO	**50.00%**	12
Cybersecurity Researcher	**20.83%**	5
Personnel from another federal program (NSA, DOE/ESNet, etc.)	**0.00%**	0
Other	**20.83%**	5
Total Respondents: 24		

Q2 How would you characterize your job in relationship to cybersecurity? Please check all that apply.

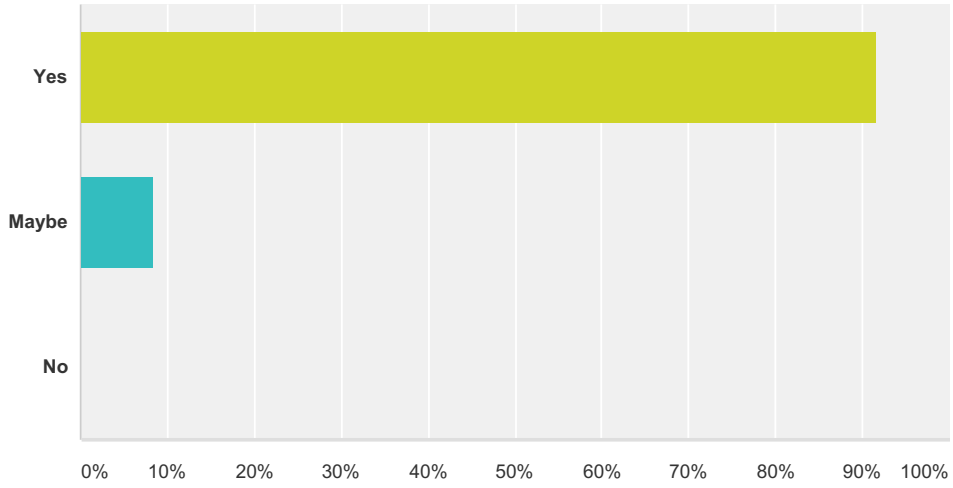
Answered: 24 Skipped: 0



Answer Choices	Responses	
I am a cybersecurity professional	**41.67%**	10
I am a technical professional who has knowledge of cybersecurity	**33.33%**	8
I have management responsibility for cybersecurity	**37.50%**	9
Other (please specify)	**16.67%**	4
Total Respondents: 24		

Q3 Based on your overall experience with the August 16 training sessions, would you participate in training offered at future summits?

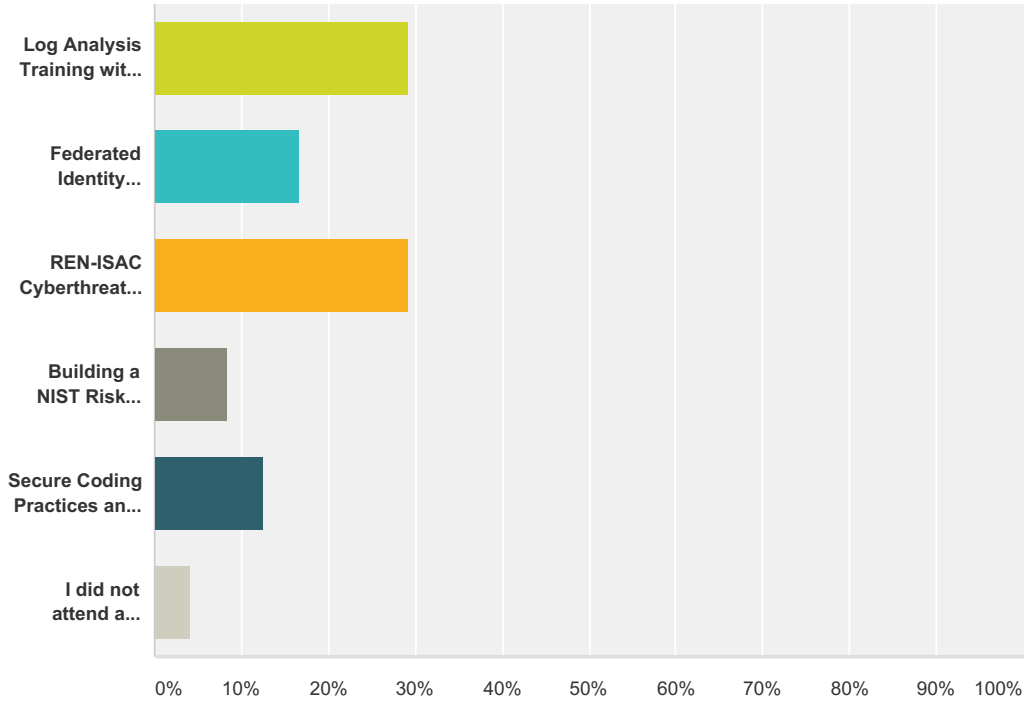
Answered: 24 Skipped: 0



Answer Choices	Responses	
Yes	**91.67%**	22
Maybe	**8.33%**	2
No	**0.00%**	0
Total		**24**

Q5 Which morning session did you attend?

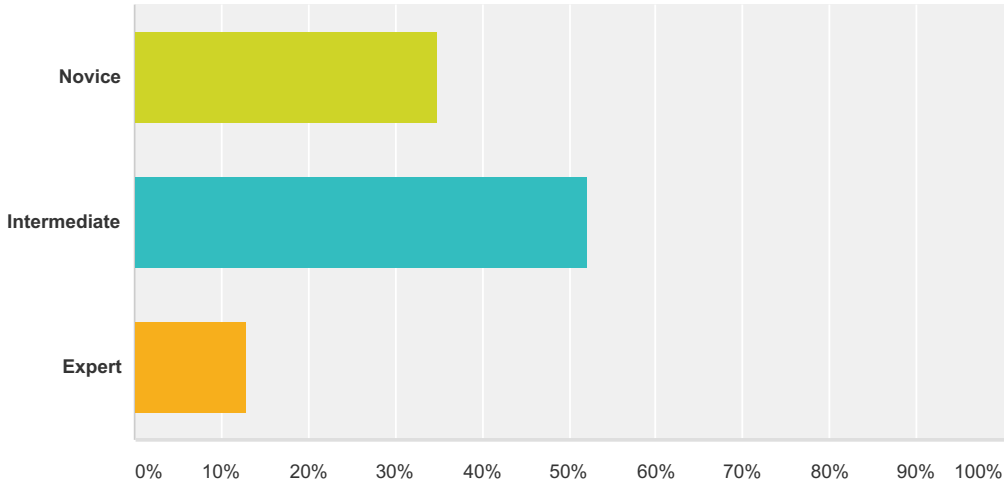
Answered: 24 Skipped: 0



Answer Choices	Responses	
Log Analysis Training with CTSC and Bro (Vlad Grigorescu, Warren Raquel, Adam Slagell, Jeannette Dopheide)	29.17%	7
Federated Identity Management for Research Organizations (Jim Basney & Scott Koranda)	16.67%	4
REN-ISAC Cyberthreat Training (Kim Milford & Todd Herring) / Developing Cybersecurity Programs for NSF Projects (CTSC TEAM)	29.17%	7
Building a NIST Risk Management Framework for HIPAA and FISMA Compliance (Anurag Shankar)	8.33%	2
Secure Coding Practices and Automated Assessment Tools (Barton P. Miller & Elisa Heymann)	12.50%	3
I did not attend a morning session	4.17%	1
Total		**24**

Q6 How would you rate your level of pre-training familiarity with the topics covered by this morning training session?

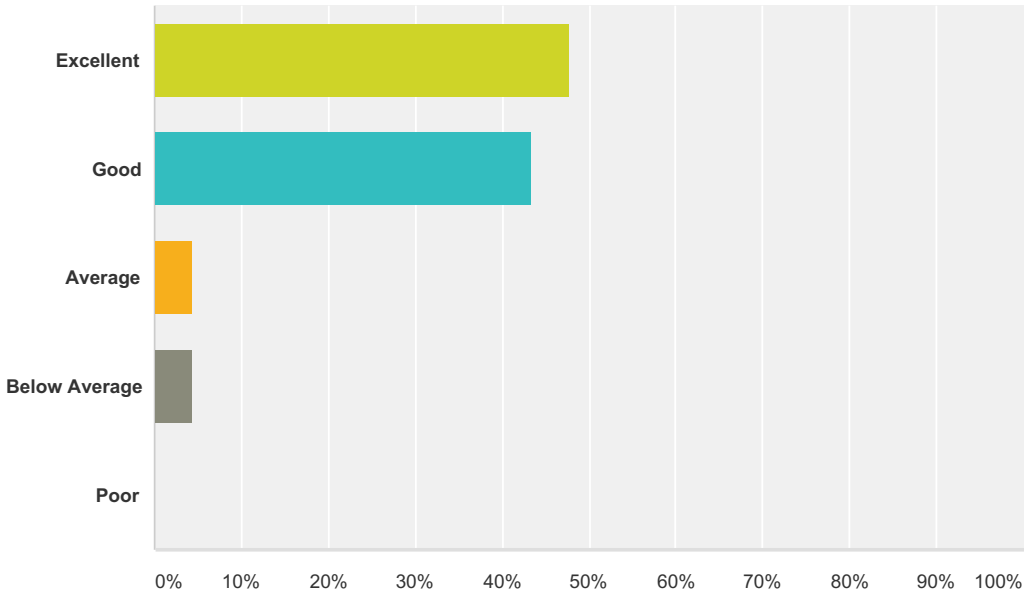
Answered: 23 Skipped: 1



Answer Choices	Responses	
Novice	**34.78%**	8
Intermediate	**52.17%**	12
Expert	**13.04%**	3
Total		**23**

Q7 How would you rate your overall experience with the morning training?

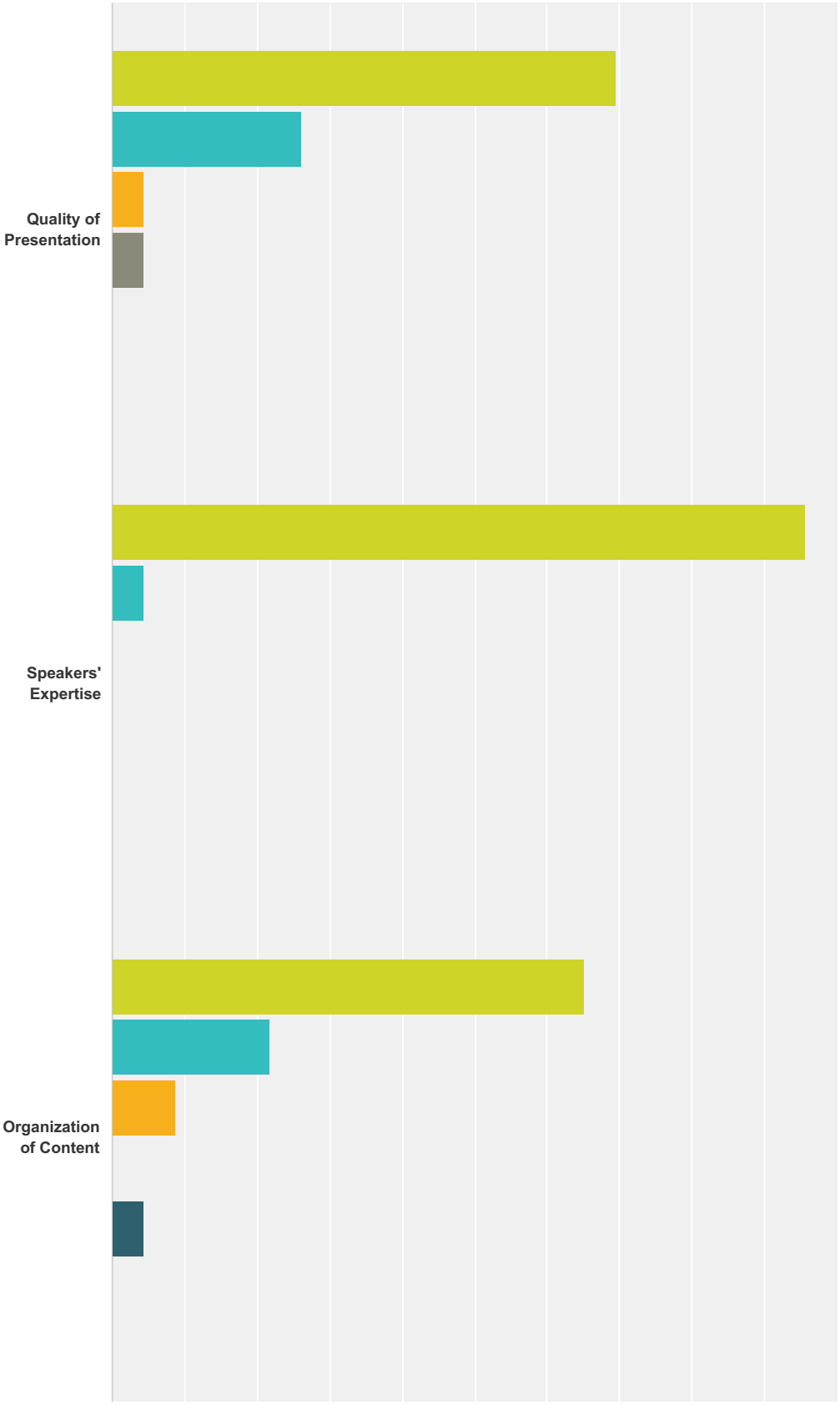
Answered: 23 Skipped: 1

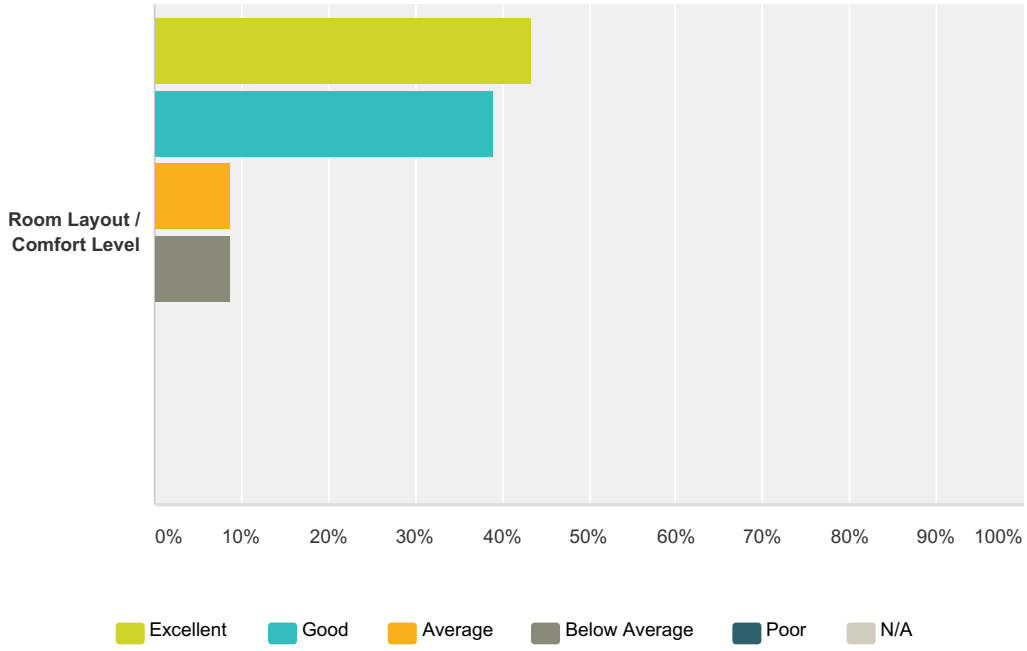


Answer Choices	Responses	
Excellent	**47.83%**	11
Good	**43.48%**	10
Average	**4.35%**	1
Below Average	**4.35%**	1
Poor	**0.00%**	0
Total		**23**

Q8 Please rate your experience with the morning training in these areas:

Answered: 23 Skipped: 1

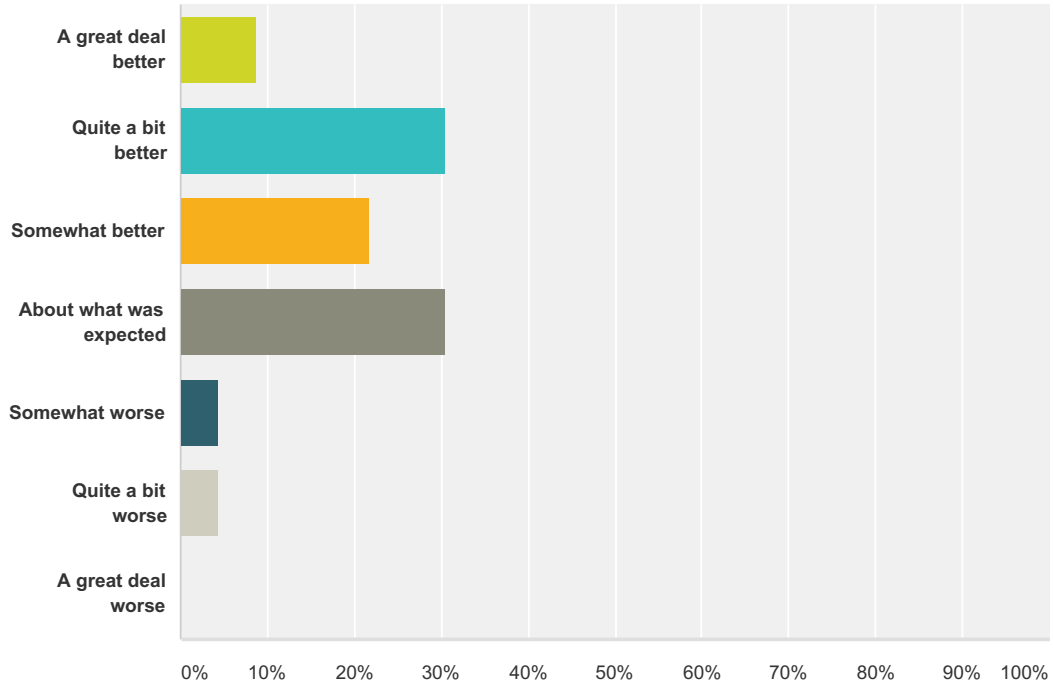




	Excellent	Good	Average	Below Average	Poor	N/A	Total Respondents
Quality of Presentation	**69.57%** 16	**26.09%** 6	**4.35%** 1	**4.35%** 1	**0.00%** 0	**0.00%** 0	23
Speakers' Expertise	**95.65%** 22	**4.35%** 1	**0.00%** 0	**0.00%** 0	**0.00%** 0	**0.00%** 0	23
Organization of Content	**65.22%** 15	**21.74%** 5	**8.70%** 2	**0.00%** 0	**4.35%** 1	**0.00%** 0	23
Room Layout / Comfort Level	**43.48%** 10	**39.13%** 9	**8.70%** 2	**8.70%** 2	**0.00%** 0	**0.00%** 0	23

Q9 Was this morning training better than what you expected, worse than what you expected, or about what you expected?

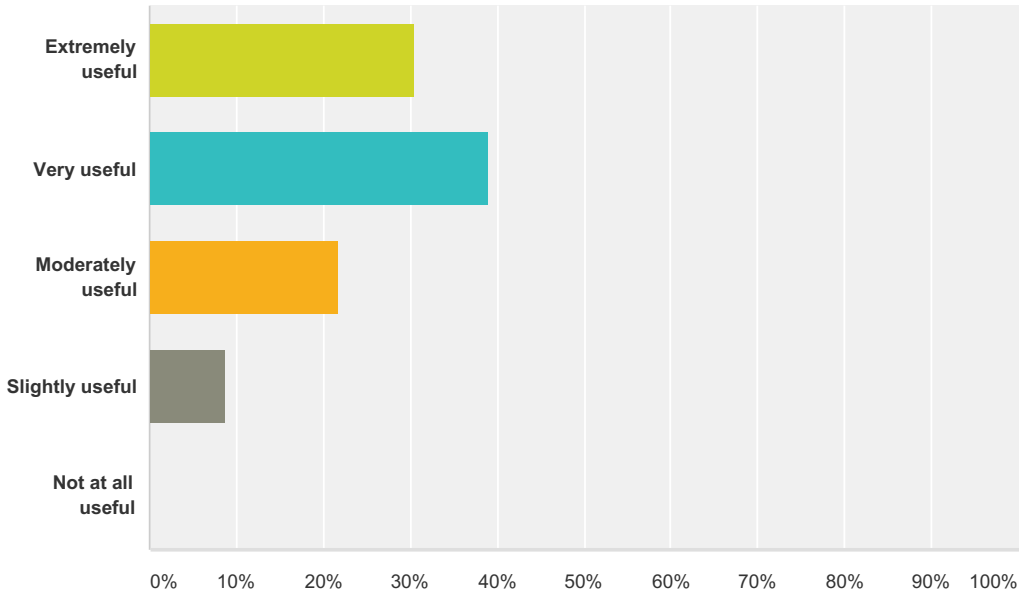
Answered: 23 Skipped: 1



Answer Choices	Responses	
A great deal better	**8.70%**	2
Quite a bit better	**30.43%**	7
Somewhat better	**21.74%**	5
About what was expected	**30.43%**	7
Somewhat worse	**4.35%**	1
Quite a bit worse	**4.35%**	1
A great deal worse	**0.00%**	0
Total		**23**

Q10 How useful to your work was this morning training?

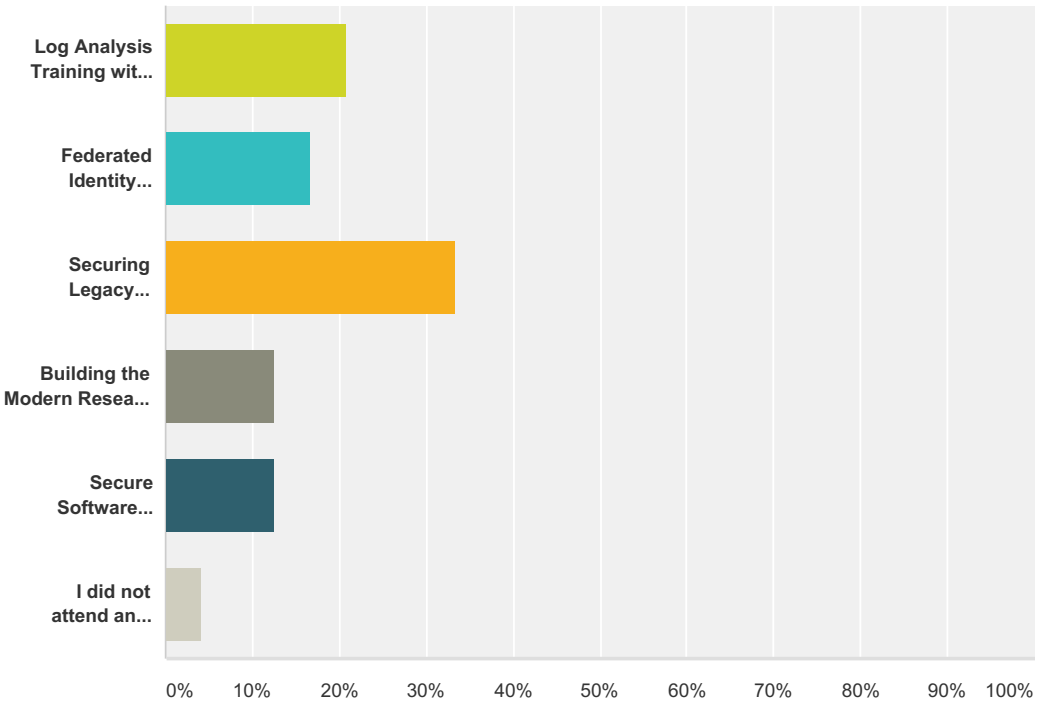
Answered: 23 Skipped: 1



Answer Choices	Responses	
Extremely useful	30.43%	7
Very useful	39.13%	9
Moderately useful	21.74%	5
Slightly useful	8.70%	2
Not at all useful	0.00%	0
Total		23

Q13 Which afternoon session did you attend?

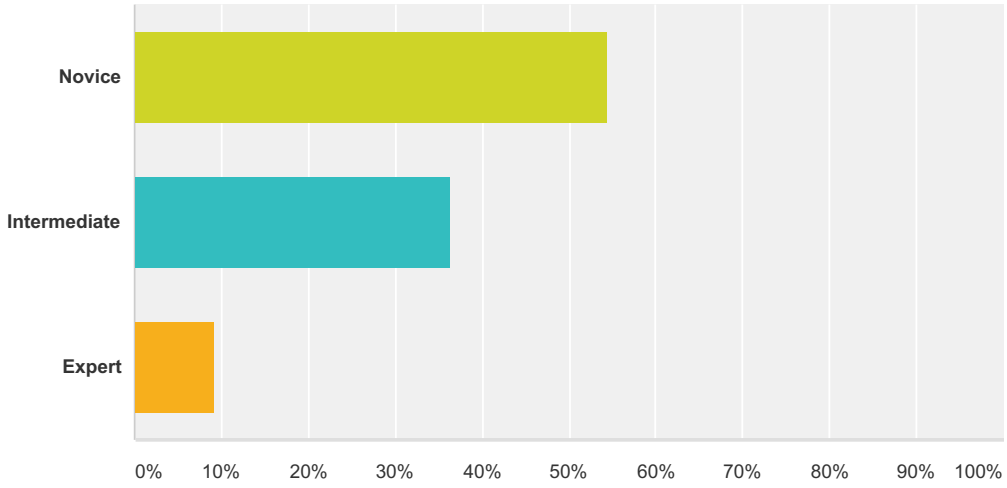
Answered: 24 Skipped: 0



Answer Choices	Responses	
Log Analysis Training with CTSC and Bro (Vlad Grigorescu, Warren Raquel, Adam Slagell, Jeannette Dopheide)	20.83%	5
Federated Identity Management for Research Organizations (Jim Basney & Scott Koranda)	16.67%	4
Securing Legacy Industrial Control Systems (Phil Salkie)	33.33%	8
Building the Modern Research Data Portal Using the Globus Platform (Steve Tuecke)	12.50%	3
Secure Software Engineering Best Practices (Randy Heiland & Susan Sons)	12.50%	3
I did not attend an afternoon session	4.17%	1
Total		**24**

Q14 How would you rate your level of pre-training familiarity with the topics covered by this afternoon training session?

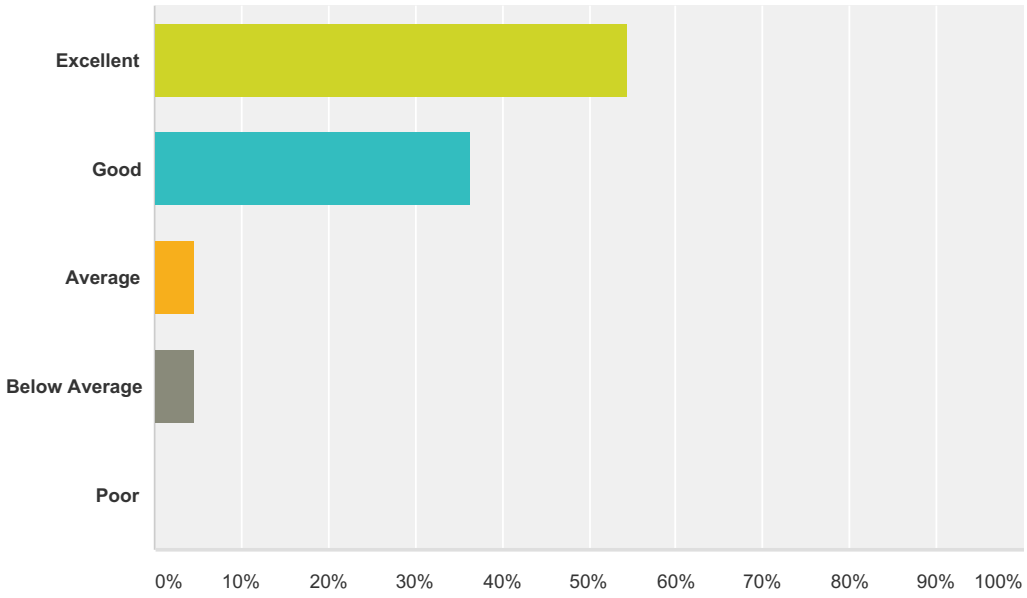
Answered: 22 Skipped: 2



Answer Choices	Responses	
Novice	**54.55%**	12
Intermediate	**36.36%**	8
Expert	**9.09%**	2
Total		**22**

Q15 How would you rate your overall experience with the afternoon training?

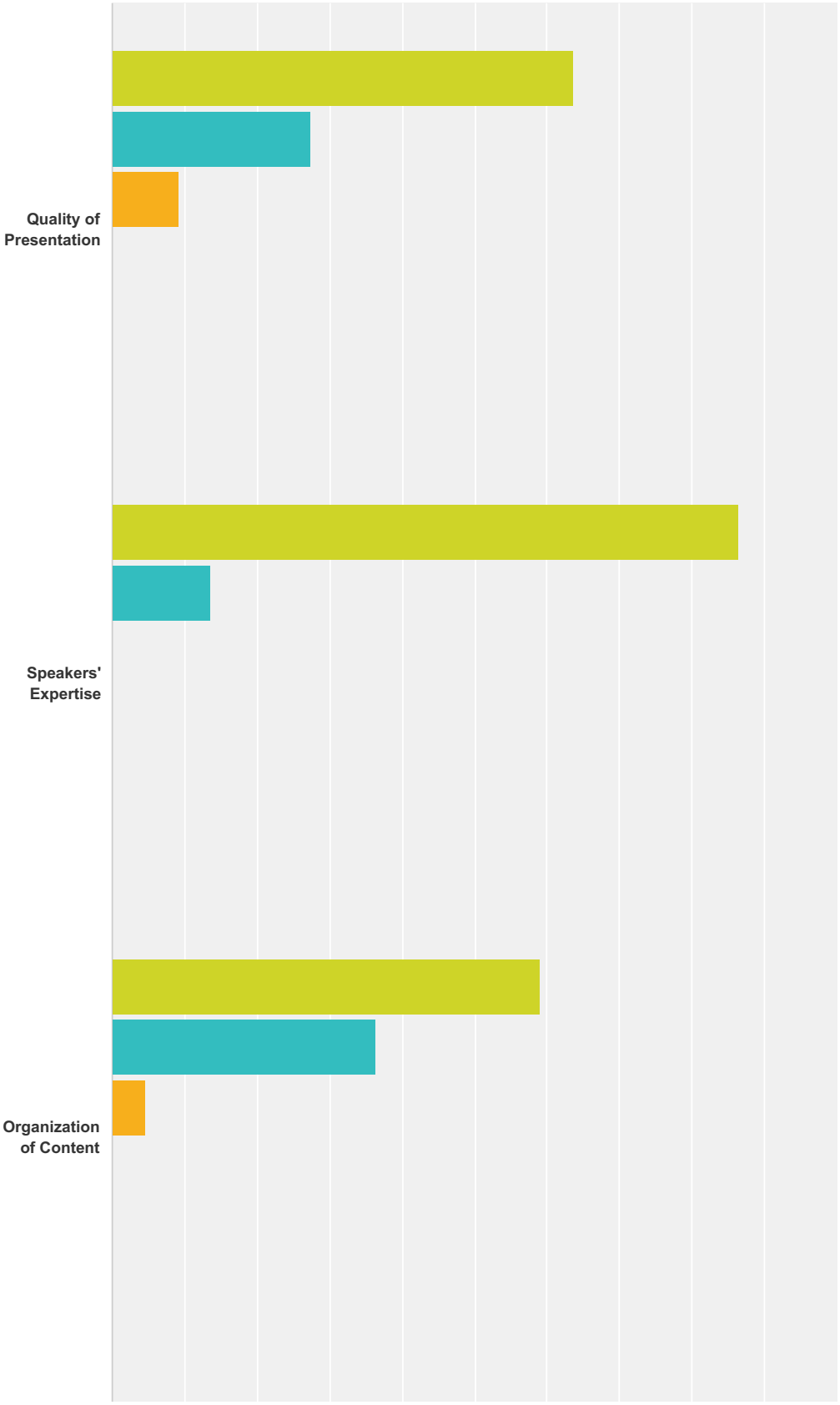
Answered: 22 Skipped: 2

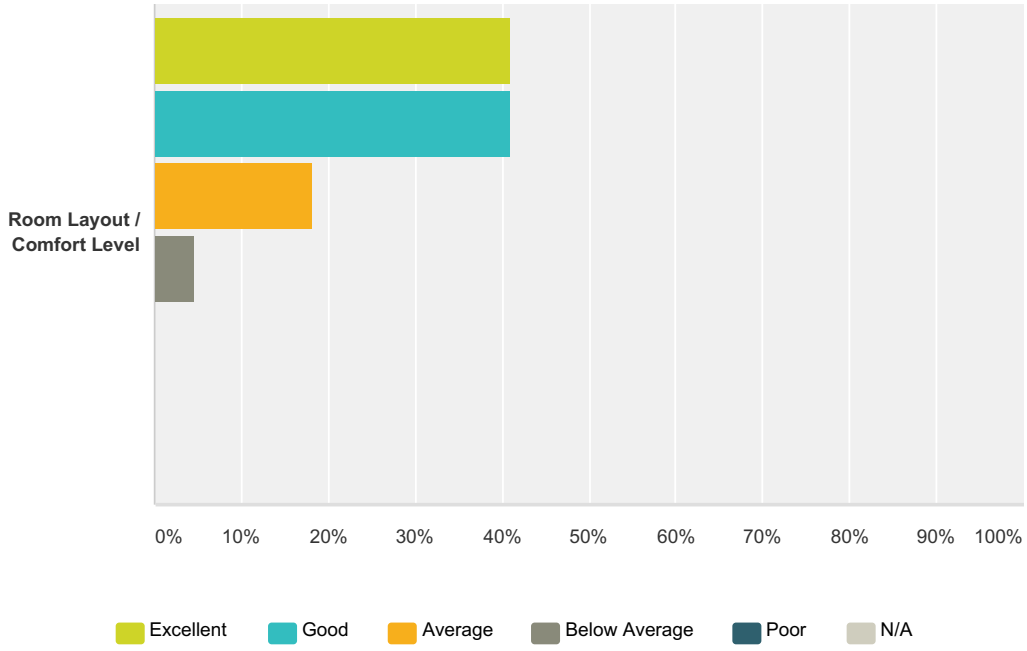


Answer Choices	Responses	
Excellent	**54.55%**	12
Good	**36.36%**	8
Average	**4.55%**	1
Below Average	**4.55%**	1
Poor	**0.00%**	0
Total		**22**

Q16 Please rate your experience with the afternoon training in these areas:

Answered: 22 Skipped: 2

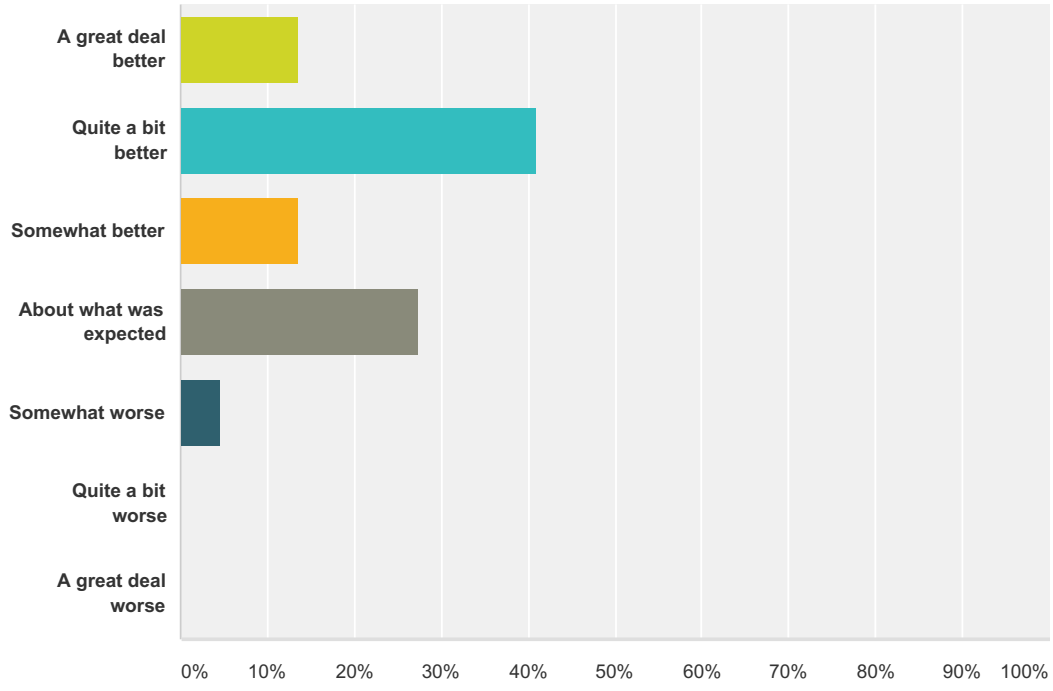




	Excellent	Good	Average	Below Average	Poor	N/A	Total Respondents
Quality of Presentation	**63.64%** 14	**27.27%** 6	**9.09%** 2	**0.00%** 0	**0.00%** 0	**0.00%** 0	22
Speakers' Expertise	**86.36%** 19	**13.64%** 3	**0.00%** 0	**0.00%** 0	**0.00%** 0	**0.00%** 0	22
Organization of Content	**59.09%** 13	**36.36%** 8	**4.55%** 1	**0.00%** 0	**0.00%** 0	**0.00%** 0	22
Room Layout / Comfort Level	**40.91%** 9	**40.91%** 9	**18.18%** 4	**4.55%** 1	**0.00%** 0	**0.00%** 0	22

Q17 Was this afternoon training session better than what you expected, worse than what you expected, or about what you expected?

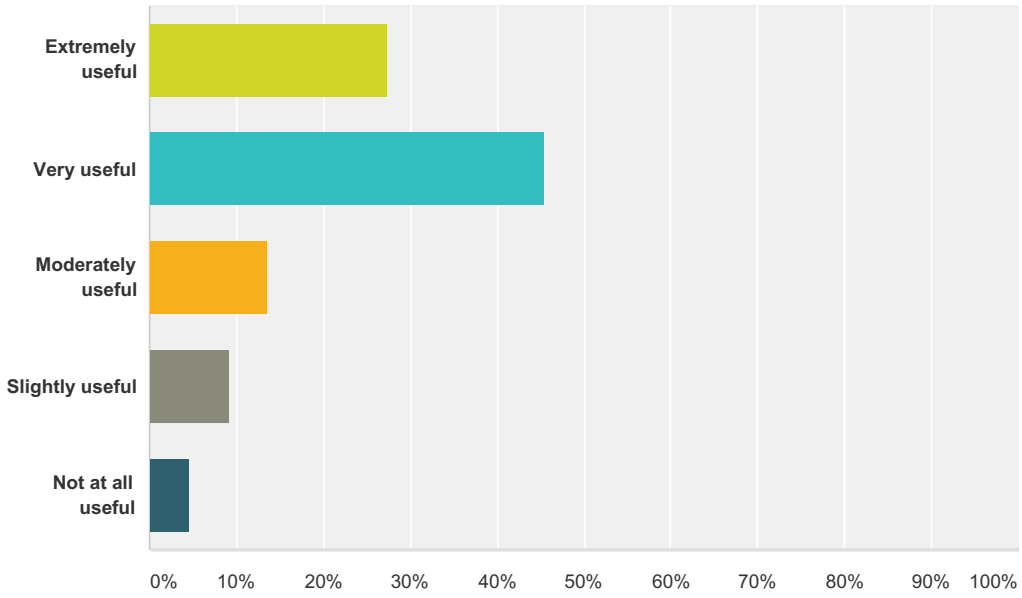
Answered: 22 Skipped: 2



Answer Choices	Responses	
A great deal better	13.64%	3
Quite a bit better	40.91%	9
Somewhat better	13.64%	3
About what was expected	27.27%	6
Somewhat worse	4.55%	1
Quite a bit worse	0.00%	0
A great deal worse	0.00%	0
Total		22

Q18 How useful to your work was this afternoon training?

Answered: 22 Skipped: 2



Answer Choices	Responses	
Extremely useful	**27.27%**	6
Very useful	**45.45%**	10
Moderately useful	**13.64%**	3
Slightly useful	**9.09%**	2
Not at all useful	**4.55%**	1
Total		**22**

Appendix H
Submitted White Papers / CFP Responses

A Secure Optical Fusion and Received-Signal-Strength-Indicator (RSSI) Approach for Threat Detection in Large Facilities

Kaiqi Xiong
Florida Center for Cybersecurity
University of South Florida
Tampa, FL 33620 USA

Security and terrorist attacks have become prominent concerns in the nation. Potential "soft targets" include hospitals, schools, retail malls, transit systems, amusement parks and sport arenas, in addition to military facilities, e.g., recent terrorism attacks at the Brussels Airport in Belgium. The nature of these targets makes them very vulnerable. Target tracking through distributed camera systems is fundamental in video and sensing surveillance and it presents a grand challenge in maintaining the identification and directionality of the target. Many approaches have been researched to address the directionality and maintenance of the tracking system including track-to-track fusion. A major challenge in tracking systems through cameras is when the target of interest moves outside of the field-of-view (FOV) due to obscurity. To maintain video tracking, researchers have mainly suggested two approaches.

- Estimation techniques such as nonlinear Kalman filters and unscented filters have been used to retain the track of the target of interest. However, such tracking may be very inaccurate when *the target of interest is an intruder.*

- Wi-Fi enabled device tracking through Received-Signal-Strength-Indicator (RSSI) is also proposed to track the target of interest. However, Wi-Fi tracking poses a challenge as environmental factors can distort the signal strength and sensors have computing and storage constraints. These influences create ambiguous results that are mixed with various security attacks to inaccurate location. We have recently addressed the above challenges on the nonlinear target tracking for threat detection where some collected data are altered by intruders through various security attacks that may include: (1) the interest of target is an intruder, (2) the part of sensor nodes is compromised by intruders, and (3) some collected data are altered during data transmissions. Specifically, the objective of this presentation is to share our development of an efficient and *attack-resilient* multiple-target tracking framework for threat detection in urban surveillance by using the Dynamic Data-Driven Application Systems (DDDAS)-based approach under computing and storage constraints. The DDDAS-based attack-resilient framework consists of two components: (1) attack- resilient multiple-target tracking pre-processing and delay-guaranteed communications by using optical fusion and RSSI, and (2) DDDAS-based decision making for threat detection by developing attack-resilient filtering techniques into dynamic data analysis. The DDDAS-based attack-resilient framework with resulting algorithms will be evaluated on the Global Environment for Network Innovations (GENI) infrastructure,

sponsored by National Science Foundation (NSF). This research aims to build security solutions for threat detection in national critical large facilities. City-scale deployment will place greater demands also on the usability of the security solutions.

Interest of Attendance

Dr. Xiong would like to take the opportunity to share his above research experience with attendees, learn the state of the arts in large facility security from other attendees, and, in particular, explore the potential to collaborate with other researchers in the field.

Brief Bio

Dr. Xiong is currently an Associate Professor at the University of South Florida. Before returning to academia, he has worked in IT industry for several years where he received the Invention Achievement Award, the Publication Award from IBM and patents. His current research interests include secure nonlinear target tracking for threat detection in large facilities and critical infrastructures, Software-Defined Networking, Infrastructure, and Exchange (SDN/SDI/SDX) for attack-resilient next-generation smart cities, computer security, secure cloud computing, and secure connected vehicles. He has published more than 90-refereed papers in leading journals and conference proceedings including ACM and IEEE transactions. NSF, BBN/NSF, AFRL, ONR, Cisco, Ericsson, and Amazon AWS have sponsored his recent research including two NSF-US Ignite grants on the development of secure SDN based communication systems for emergency responses and power grids, respectively. He also organized and co- organized a number of conferences and workshops including three Global Environment for Networking Innovations (GENI) Research and Educational Experiment workshops and three workshops on Computer and Networking Experimental Research Using Testbeds, co-located with ICNP2014, ICDCS2015, and INFOCOM2016.

Cybersecurity Budgeting

A Survey of Benchmarking Research and Recommendations to Organizations

Scott Russell, Postdoctoral Fellow, Indiana University Center for Applied Cybersecurity Research
Craig Jackson, Chief Policy Analyst, Indiana University Center for Applied Cybersecurity Research
Bob Cowles, Principal, Brightlite Information Security

Draft Submitted to 2016 NSF Cybersecurity Summit Program Committee 10 June 2016

Abstract

A common starting point for organizational budgeting is benchmarking research. These studies effectively answer the question: "What are the Johnson's doing?" We have conducted an exhaustive review and analysis of cybersecurity budgeting benchmark research (including more than 50 studies). This paper offers a bird's eye view analysis of the available research and its quality, and provides recommendations to organizations on whether and how to utilize this research as well as recommendations for improving future research.

1 Introduction

We set out to identify research studying quantitative metrics that can be employed to assess an organization's cybersecurity program, beginning with the most readily available and logical metric to follow: money. Specifically, how much money do organizations spend on cybersecurity? Spending is a concrete number; it theoretically correlates with improved security; and it is comparatively easy to study in a domain where usable metrics seem to elude our grasp. Perhaps most importantly, board members and C-suite officers understand money, which often cannot be said for more complex methods for testing security. Despite the seemingly straightforward nature of this question, our analysis found the state of the cybersecurity budget research sorely lacking. Information relating to cybersecurity budgets is rarely presented in a verifiable and actionable manner, and even when presented as such, cybersecurity budgets contain a host of complexities that must be understood and addressed for the data to be practically implemented.

2 Methodology

To conduct our review we queried for research returning a combination of the words "cyber," "IT," "network," or "information" and "security"[1] with "spending" and/or "budget." Based on these results, we conducted a preliminary analysis of the studies presented, looking for independent reviews that collected and analyzed new data (as opposed to reporting other work), or those that compiled research found in other sources. Among those sources, we then narrowed the pool based on select criteria,

---

[1] This included obvious variations, such as hyphenations, so the term "cybersecurity" would also warrant "cyber security" and "cyber-security." For completeness, we also included redundant terms, such as "IT cybersecurity" and "network cybersecurity."

2.1 Quantitative Research

The primary criterion was the presence of at least one quantitative metric for assessing organizational cybersecurity spending. This primarily was satisfied by studies assessing cybersecurity spending as a percentage of total IT budget, as a percentage of total revenue, or as a dollar amount. We excluded surveys asking solely whether companies' cybersecurity spending was "increasing, decreasing, or remaining the same." Although arguably quantitative, this information is of little direct use without a reference point for from what baseline the budget is increasing or decreasing,[3] and without discussion of how the budget was quantified.[4] We also excluded research that quantified or forecasted the "cybersecurity market" generally, without new data about the specific spending practices of organizations.

2.2 Published Methodology

We excluded studies that did not publish their methodology, as this prevented our effective assessment of the study's veracity. This therefore excluded private studies for which press releases announced findings, but which are not made fully available, as these results present insufficient information to assess methodology.

2.3 Publicly Available

This review is limited to studies that are publicly available or available through the services provided by a typical university library.[5] This includes research that is only made available after providing an email or other contact information, but does not include any research that requires payment or the production of a credit card number to access.

2.4 Time Period

Finally, this review is limited to studies published between January 2011 and February 2016. For reviews that are conducted yearly, we limited our analysis to the most recently published version of each yearly review.[6]

---

[2] For our purposes, we excluded budgetary analyses of national budgets, as well as the budgets of international bodies like the European Union. [3] An increasing budget may reflect inadequate spending in previous years, whereas a decreasing budget may represent overspending.

[4] An "increasing" budget represented in dollars may be a static budget as a percentage of IT budget, reflecting overall growth of the company or adjustment for inflation, whereas a shift in budget as a percentage of IT budget cannot be properly interpreted without inclusion of any shifts in the total IT budget. A decreasing IT budget coupled with a proportionately smaller decrease in cybersecurity spending would manifest as an increasing cybersecurity budget as a percentage of IT budget.

[5] Our research included studies obtained through the Indiana University Library system. [6] The reasons for this were twofold: first, the most recently published review is often the only one made available by these research firms, making that data the most applicable to what a private company would be able to find; second, inclusion of each yearly study would skew the overall data towards the research methods of the firms that conduct yearly reviews, and diminish the relative weight of non-annual reviews.

3 Results

Relying upon the above criteria, we collected over 50 studies presenting independently gathered data. We then narrowed the pool to 11 surveys which met all of the criteria specified, of which 8 represented broad spectrum reviews, and 3 represented sector-specific reviews. Of the 5 studies that quantified spending as a percentage of IT budget, the results suggest that the majority of budgets lie within the range of 3% and 12% of IT budget, with 3.8% [PWC],[7] 8.2% [Ponemon/Dell],[8] 5.1% [Gartner],[9] 7.5% [Wisegate],[10] and 12% [CIO Magazine][11] as the reported global averages.[12] Three additional studies did not provide a global average, instead opting to present solely a graphical overview of all data collected, providing spending ranges as a percentage of IT Budget [SANS][13][EMC],[14] and as dollar amounts [EY].[15] Considering that each of these studies defaults toward presenting their data as an overall average, greater subdivision based upon important factors, such as sector and size, may indicate an even larger range of 2%-14%. Below, we discuss this in greater detail. With regard to organizational size,[16] Wisegate found that the average cybersecurity budget for small companies was 10% of IT budget, whereas the average budget for large companies was only 4% of IT Budget.[17] PWC similarly acknowledged the importance of organizational size as a factor in cybersecurity budgets, although in-depth analysis was only provided for the "Finance" sector, where small organizations averaged 14.7% of IT Budget, as compared with 3.7% for large organizations.[18] SANS also found a strong influence of organization size on budget, showing a trend of increased

---

[7] [PWC] "The Global State of Information Security® Survey 2015", PwC, 2015. [Online]. Available: http://www.pwccn.com/home/eng/rcs_info_security_2015.html. Accessed on: Jun. 10, 2016. [8] [Dell]"2015 Global IT Security Spending & Investments Report", Dell, 2015. [Online]. Available: http://www.dell.com/learn/us/en/uscorp1/press-releases/2015-06-08-dell-secureworks-and-ponemon-institute. Accessed on: Jun. 10, 2016.

[9] [Gartner]"Don't Be the Next Target - IT Security Spending Priorities 2014", Gartner, 2015. [Online]. Available: http://www.gartner.com/document/2703221?ref=TypeAheadSearch&qid=5dbf48ee96bb217914bff14d0927e39e. Accessed on: Jun. 10, 2016. [10] [Wisegate] M. Zainach, "2013 IT Security Benchmark Report," Wisegate. 2013. [Online]. Available: http://wisegateit.com/resources/downloads/wisegate-security-benchmark-report.pdf?_ga=1.104382208.1637083132.1434031731. Accessed on: Jun. 10, 2016.

[11] [CIO] "2016 State of the CIO", CIO, 2016. [Online]. Available: http://core0.staticworld.net/assets/2016/01/14/2016-state-of-the-cio-executive-summary.pdf. Accessed on: Jun. 10, 2016. [12] This does not include respondents who selected "Unsure." [13] [SANS] B. Filkins, "IT Security Spending Trends," SANS, 2016. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697. Accessed on: Jun. 10, 2016. [14] [EMC] "IT Security Survey 2014", EMC. 2014. [Online]. Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=139455&Itemid=2926. Accessed on: Jun. 10, 2016. [15] [EY] "Global Information Security Survey 2014", EY, 2015. [Online]. Available: http://www.ey.com/GL/en/Services/Advisory/EY-global-information-security-survey-2014. Accessed on:Jun. 10, 2016. [16] The exact definitions of "large," "medium," and "small" companies, or their relevant analogues, varied across the studies. [17] See, [Wisegate] supra. [18] See, [PWC] supra.

security budgets as a percentage of IT budgets for smaller organizations.[19] Similar trends in other sectors can be identified through data exploration tools provided by PWC and EY.
With regard to sector, Wisegate showed substantial variation in spending based on sector, ranging from 10.4% in "Banking and Financial Services" to 2.3% in "Government," despite a global average of 7.5%. [20] Similarly, PWC found spending ranging from 3.7% with "Healthcare, Retail, and Technology," up to 6.9% with "Industrial Products."[21] E&Y, while not providing in-depth analysis, provides access to the raw data, differentiated by sector, which further suggests considerable sector-specific variations in spending.[22] In a sector-specific study, SANS found that cybersecurity spending in the "Healthcare" sector was 1-3% of IT budget for 15% of respondents, with slightly less than 10% spending more than 10% of IT budget, and slightly over 10% spending less than 1% of IT budget.[232425]

4 Analysis

4.1 Overview

Based on the foregoing, we can conclude that the research suggests a great deal of variability in cybersecurity budgeting, both within studies and between studies, and that greater subdivision of the data based upon sector, size, and other variables is appropriate to derive meaningful results. While the global averages identified in each of the studies lay broadly in the range of 3% and 12% of IT budget, the large variability in the findings coupled with the lack of a clearly stated standard deviation make drawing any strong conclusion from these values ill-advised. Despite this variability in global averages, the research does suggest that sector and size have a strong influence on cybersecurity budgets, warranting more in-depth analysis.

4.2 Organizational Size

Our research suggests that organizational size has a notable impact on cybersecurity budgets.[26] Each of the non-excluded studies that differentiated the data based on organization size identified a trend toward proportionate reductions in spending with increasing size. Although the delineation of sizes varied among

---

[19] See, [SANS] supra. [20] See, [Wisegate] supra. [21] See, [PWC] supra. [22] See, [EY] supra. [23] B. Filkins, "New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations", SANS. 2014. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/threats-drive-improved-practices-state-cybersecurity-healt h-care-organizations-35652. Accessed: Jun. 10, 2016. [24] Note, however, that 47% were unsure of their company's cybersecurity budget. [25] As a point of comparison, there is also a series of sector-specific studies conducted by Frost and Sullivan, which are addressed separately because the specific metric studied was "network security," which is arguably distinct from overall "cybersecurity," and because the results are notably outside the range found by the remainder of the studies. This series of studies found in "Healthcare," "Banking/Financial/Insurance," and "Manufacturing," the average percent of IT Budget devoted to "network security" was 16%, whereas for "Government" it was 19%, and for "Retail" it was 15%. Considering the substantial departure from other studies, the variability in terminology, and the unavailability of detailed methods, this study is not included with the other studies, but given the usage of spending as a percentage of Total IT Budget, (a relative rarity), and the strong reputation of the group conducting the study, it is included for completeness. See, e.g., "The Future of IT in the Manufacturing Industry", F&S. 2014. [Online]. Available: http://cds.frost.com/p/71559/#!/ppt/c?id=M9D2-01-00-00-00. Accessed on; Jun. 10, 2016. [26] Although additional factors are often speculated to have an impact upon cybersecurity budgets, such as maturity and geographic region, the data as yet is insufficient to make any definitive statements.

studies, there nonetheless exists a consistent negative association between organizational size and spending as a percentage of IT budget. We believe this is a logical consequence of larger organizations enjoying economies of scale. This trend suggests certain baseline costs for a cybersecurity program that organizations incur regardless of their size, after which the program costs grow more slowly than the IT budget.

4.3 Sector

Similarly, our research suggests that an organization's sector has a substantial impact on cybersecurity budgets. Each of the non-excluded studies that differentiated by sector identified notable spending variations between those sectors. Despite, again, a lack of uniformity in delineating sectors, certain trends are nonetheless identifiable from the data presented. "Finance" and "Aerospace and Defense," both of which are consistently differentiated, are also consistently identified as employing higher than average cybersecurity spending, whereas "Retail," another recurrent category, was consistently lower than the overall average. The lack of more consistent delineation between sectors makes any further conclusions difficult, although emerging trends may be speculated based upon individual studies and sector-specific cyber-risk.

4.4 Limitations

Notwithstanding these trends, our analysis of the study of cybersecurity budgets as a whole found several foundational problems that made drawing any strong conclusions from the available research difficult. Indeed the exclusion criteria we applied left few studies remaining, and even among the best designed of these remaining studies, elements of their methodology and results cast doubts as to their overall utility.

4.4.1 Missing Baseline Data

The most recurrent problem, highlighted in Section 2.1, was that studies frequently looked exclusively at relative changes in cybersecurity spending, without any baseline for comparison. Surveys asking whether cybersecurity spending is "increasing, decreasing, or remaining the same," litter the headlines, and yet provide little actionable information, particularly to an organization first attempting to budget cybersecurity. Without some knowledge of what the individual budgets are shifting from, this information amounts to answering the question "How much should I spend on cybersecurity?" with "More!" While some of the non-excluded studies began to address this concern by providing more complete data,[27] this proved to be the exception, and not the rule.

4.4.2 Survey Methodology and Rigor

Even among the studies that were not excluded, the overarching reliance on survey data inserts a great deal of uncertainty as to the accuracy of the responses the data is based upon. Considering the variability in the individual respondents' positions within the surveyed companies, the generally low response rates, and the prevalence of "unsure" answers, it is difficult to say whether the information about budgets reflects what budgets are, or what individuals guess the budgets are. Coupled with this is the recurrent failure to clearly and consistently define what constitutes "cybersecurity," both from the variability in terminology (e.g., information security vs. cybersecurity), as well as the frequent overlaps between cybersecurity and other budgetary areas.[28] Indeed even the delineation of "IT budget" may vary between

[27] See, [SANS] supra. [28] This may include overlaps with identity management, physical security, code hygiene and coding

best practices,

sectors, potentially undermining this as a point of comparison. Even assuming consistency, the exclusive reliance upon survey data raises the spectre of bias, whether through non-response, non-representative samples, or social desirability. While these variations may normalize in the aggregate, they nonetheless insert uncertainty into the cybersecurity budget analysis.

4.4.3 Hidden Variables

Moreover, cybersecurity budgets are influenced by a number of factors, many of which were unstudied or unidentified in our sample, that can greatly alter how an individual organization interprets the data. Although the influence of sector and size are well established, and frequently differentiated, other factors, such as the maturity of the cybersecurity program or the geographic region of the organization, are rarely studied in any meaningful way. For example, although programmatic maturity is frequently discussed as a potential confounding factor, (more mature cybersecurity programs could logically operate more efficiently), the direct impact of cybersecurity program maturity was only directly identified in one study. Wisegate found that more mature programs tended to have higher budgets.[29] Whether this is indicative of a larger trend is unclear, as companies with more mature cybersecurity programs may also fit into demographic groups that are associated with higher spending, such as the finance sector. Nevertheless, the debate surrounding cybersecurity maturity highlights the importance of gathering and analyzing as many factors as possible, as consideration of these additional factors can greatly alter individual organizations' budgetary analyses.

4.4.4 Intra-study Variability

However, the single most troubling caveat to the available data is the massive intra-study variability reflected in the data, even when taking into account sector and size. PWC found that 3.92% of "large businesses" (total revenues exceeding $1 billion) selected the lowest bracket of spending for information security, $49,000 or less, while 1.1% of small businesses (total revenues less than $100 million) selected the highest bracket of spending for information security, at $10 million or more.[30] Similar variability was found in all studies which provided granular data, with Dell finding that 7% of companies spent over 30% of IT Budget on IT Security;[31] and E&Y finding that among businesses with revenues over $10 billion, between 18% and 29% spend less than $1 million on information security, including 24% of businesses with total revenues between $25 and $50 billion.[32] While these outliers may simply reflect inaccurate responses, all organization sizes and sectors appear to be represented in all budgetary brackets to some degree in each survey, suggesting either a massive degree of actual variability in spending, or a fundamental unreliability in the data presented.[33] Such vast variability makes it very difficult to abstract a meaningful normative baseline or average spending.

---

and the usage of third party cloud storage and services. [29] See, [Wisegate] supra. Therefore the study found the opposite of the presumed effect. Although the reasons for this are unknown, and could be many, the most logical would seem to be that subsets of an organization are unlikely to voluntarily reduce their own budget. [30] See, [PWC] supra. [31] See, [Dell] supra. [32] See, [EY] supra. [33] This is taking into account responses that amount to "unsure" or "don't know."

5 Recommendations

5.1 Recommendations for Organizations

Avoid over-reliance on benchmarking data generally. The variability in studies we reviewed (in terms of rigor, methodologies, sample size and bias, and results) strongly suggests that most benchmarking studies are of limited validity in describing the state of budgetary reality. There is even less reason to believe these studies represent what organizations should spend. Cybersecurity budgeting is a complex organizational activity. Organizations are well-advised to think carefully about their budgetary processes for cybersecurity[34] and how cyber risk intersects with organizational mission, rather than over-focus of the final numbers or percentages.

Talk to peer organizations and seek out relevant case studies, or survey studies that differentiate the data based upon, at a minimum, sector and size. Considering the importance of sector and size, as well as the variability in cybersecurity spending generally, organizations should look for the data sets that represent the most similarly situated organizations to their own. While inclusion of additional criteria is preferred, sector and size should be considered mandatory for a meaningful benchmarking. Organizations should prefer studies that provide access to all of the data, so that organizations can visualize the spectrum of spending practices among their peers. At a minimum should include access to averages among organizations of their size within their sector.

Ignore all but the highest-quality benchmarking studies. We believe PWC[35] and EY provide the most actionable data, in large part due to their release of data exploration tools to visualize and filter their data, whereas SANS and Wisegate should also be considered for broader insight into security trends generally. These studies are highlighted in particular because of their attempts to quantify important trends, their representations of the nuances of their datasets, and their insights into the underlying data.

5.2 Recommendations for Future Studies

Establish clear methodology, internally consistent definitions, and rigorous standards for the data collected.

Provide more granular access to the underlying data. Considering the importance of certain factors on spending, mere access to a global average is often misleading, and of little direct worth to an organization wishing to benchmark. By providing more granular access to the data, organizations will be better empowered to select the sample set that aligns with their own requirements.

Provide greater detail into how security budgets are allocated. Although generalized benchmarking studies are useful for high level decision-making, often organizations will be interested in specifically how much should be spent for particular security functions. For instance, how much do organizations spend on security personnel vs. technological “solutions” vs. outsourced services?

Increase methodological rigor and employ an increasing variety of research methods. Almost the polar

---

[34] See, Moore et al., “Identifying How Firms Manage Cybersecurity Investment”, 2016. [Online]. Available: http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_19-1.pdf. Accessed on: Jun. 10, 2016. [35] PWC has since released a subsequent “State of Information Security 2016,” which no longer provides spending averages as a percentage of IT budget, instead providing only a data exploration tool in dollars.

opposite of survey research, detailed case studies can provide powerful insights into complex organizational processes. This is particularly important in evolving, high variability domains.

Collect more data on potentially relevant factors (e.g., program maturity, presence of regulated data or systems) to determine whether and to what degree they relate to cybersecurity spending. Although our research has identified a select few factors which have a notable impact, it is clear that "more research is needed." Multifactor analysis is critical to making this research meaningful.

Quantify the impact of variable cybersecurity budgets on security outcomes, such as data breaches or network intrusions. An overarching shortcoming of the available data is that it represents solely what others are doing, not whether what they are doing is working. The identification of and assessment of cybersecurity metrics is highly important moving forward, as information on the security practices of others is of little worth when their security is inadequate.

Acknowledgements

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation or Indiana University. This research was supported in part by the Center for Trustworthy Scientific Cyberinfrastructure (CTSC), the NSF Cybersecurity Center of Excellence. CTSC is supported by the National Science Foundation under Grants Numbered OCI-1234408 and ACI-1547272. For more information about the Center for Trustworthy Scientific Cyberinfrastructure please visit: http://trustedci.org/.

The Science DMZ as a Security Architecture:
How the Science DMZ Enables a Risk-Based Campus Security Program

Michael Sinatra
ESnet - June 2016

Abstract

The Science DMZ architecture[1] proposes a novel method of design for network segments optimized for large-scale data transfer (LSDT) functionality. LSDT has special requirements, both in the security and functional arenas. Attempts to incorporate LSDT functionality into a more traditional perimeter security model can cause problems both with LSDT functionality, as well as weaken overall campus security. The Science DMZ attempts to solve this problem by segmenting the LSDT function away from the traditional campus security perimeter. However, insufficient attention has been paid thus far as to how the Science DMZ fits into a larger strategy of risk-based segmentation and functional maximization of campus networks. This paper examines typical risk- and control-based security approaches and proposes a framework in which the Science DMZ, combined with a larger segmentation approach, actually improves the security of valuable campus information assets, while still maximizing LSDT function and security. It concludes with some examples as to how the security of the research enterprise can be vastly improved with a Science DMZ deployment that is carefully aligned with a segmentation strategy.

Introduction

The Science DMZ design is rapidly gaining traction in the Research and Education community. Many educational and research institutions, from the US Department of Energy's National Energy Research Supercomputer Center (NERSC) to large Carnegie R1 universities, to much smaller colleges and research institutes, are all deploying some variant of the Science DMZ model.[2] The National Science Foundation has given numerous financial awards to educational institutions deploying the Science DMZ.[3] Entire confederations of Science DMZs and Data Transfer Nodes (DTNs), such as the Pacific Research Platform and proposed Atlantic Research Platform, are being established.[4] Science DMZs are quickly becoming an integral part of a campus network infrastructure.

---

[1] E. Dart, L. Rotman, B. Tierney, M. Hester and J. Zurawski, "The Science DMZ: A network design pattern for data-intensive science," *2 013 SC - International Conference for High Performance Computing, Networking, Storage and Analysis (SC)*, Denver, CO, 2013, pp. 1-10. doi: 10.1145/2503210.2503245 [2] For the prototypical Science DMZ model, see http://fasterdata.es.net/science-dmz/. [3] h ttps://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504748 contains descriptions of the various CC* grants that have been awarded by the NSF, as well as links to individual award abstracts and maps of awardees. See also Kevin Thompson's summary in h

ttp://www.thequilt.net/wp-content/uploads/KThompson_Quilt_Feb2016.pdf. [4] On the Pacific Research Platform (PRP), see http://prp.ucsd.edu/. Both the PRP and the proposed Atlantic Research Platform are described in the 2016 issue of the Quilt Circle. See https://issuu.com/noahredman1/docs/the2016quiltcircle, especiallypp.2,7. Onpage7,theproposedAtlantic Research Platform is described as "Network-wide Science DMZ."

Still, there is much concern about how best to secure the Science DMZ. While the Science DMZ attempts to provide a bona-fide security model for LSDT, it suffers from its incompatibility with control-based security strategies that specifically posit the use of stateful perimeter-based control mechanisms such as commercial firewalls. The Science DMZ explicitly eschews these mechanisms for performance reasons, which has led to the misperception that the Science DMZ is principally concerned with "avoiding firewalls." Although the Science DMZ attempts to minimize risk by bypassing *stateful* firewalls, it is fully compatible with a default-deny security policy enforced by stateless[5] means, such as line-rate router ACLs.[6] Nevertheless, the question remains, "how to secure a Science DMZ?"

Control-based vs. Risk-based Security

I argue that questions that specifically ask how to secure a Science DMZ stem from a *control-based* view of security. Control-based security starts with a set of controls which are assumed (but generally not verified) to improve the security of a set of valuable assets and reduce risk, both to said assets and the institution managing them. Control-based security strategies tend to focus on technology and on top-down security policies and checklists. Security and risk are audited by examining the *presence* of certain key controls, without actually verifying that they are reducing risk commensurate with their total cost, including the costs of potentially reduced functionality for the assets being protected by the controls.

The advantage of control-based security is that it is labor-saving over other types of security. Having a ready set of controls that are assumed to provide security yields a short-cut that allows minimal security and risk-assessment staff to still provide potentially substantial security benefits to a large set of campus resources. In particular, a large, stateful perimeter firewall, while expensive in terms of capital costs, can provide benefits to large portions of a campus with minimal managerial overhead.

The disadvantage of control-based security is that it lends itself to a one-size-fits-all security policy, which ignores the wide diversity of information assets, and concomitant risk profiles, present on modern university or research lab campus. While it potentially saves money in the near term, it ultimately reduces efficiency: Controls are applied to resources whether or not the controls reduce risk, and more controls are assumed to provide more security, even if this is not actually the case. Although campuses have been moving more toward control-based security in recent years, it appears that data-exfiltration breaches, to cite one possible measure of security, have been steady, or possibly on the rise.[7]

---

[5] A discussion of stateful vs. stateless firewalls can be found in NIST publication 800-41, section 2.1. http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

[6] The "avoiding firewall" misperception also obscures other critical features of the Science DMZ, such as the use of high-queue-depth network interfaces for WAN connections, placement of the Science DMZ close to the campus border to reduce within-campus points of failure and degradation, and ongoing performance and security monitoring through technologies like perfSONAR and Bro. While this paper is mainly concerned with the security *f eatures* of the Science DMZ, it is drawn from the inspiration that an excessive focus on avoiding firewalls can lead to suboptimal Science DMZ deployments, if the firewall issue crowds out other important features.

[7] I discuss this in a currently-unpublished presentation titled "What's wrong with information security in higher education?" given at the Research and Education track at the North American Network Operators' Group, NANOG 60, Atlanta, GA, February 2014. My own experience with my former institution, UC Berkeley, and other UC

Control-based strategies can be contrasted with risk-based strategies. While control-based strategies attempt to short-circuit careful risk assessment, a risk-based strategy makes risk assessment the foundation of the security enterprise. Assets and resources are first assessed for their risk to both the asset itself and to the host institution, and then only once the risk assessment is complete, security controls are devised to carefully match and mitigate the identified risks.
Risk-based strategies have the disadvantage of being more labor-intensive, as risk assessments must be completed and then custom security strategies tailored to the set of identified risks. However, they can also be more efficient and more secure, as they reduce the incidence of ineffective controls being applied. Risk-based strategies may also be delegated to the owners of the resources, rather than applied solely by the campus security team. As long as proper accountability is in place and is well-understood, such delegation empowers campus IT administrators, spreads the responsibility for security, and fosters a "security culture," which can be far more effective than simple control-based security.

It is also possible to have a hybrid approach, where:

1. Risk profiles are developed for a set of resources or assets.
2. "Standard controls" are proposed, which match the risk profile.
3. "Compensating controls" are allowed through an exception process. Compensating controls mitigate the risk more effectively than the proposed standard control, and/or they preserve critical functional requirements better than the standard control.

In the hybrid model, steps 1 and 2 can be performed by the security team, while step 3 can be proposed by the resource owner, thereby spreading responsibility. The resource owner can decide whether to accept the standard control or propose a compensating control.

Segmentation and the Science DMZ

It is pretty obvious that even a mid-sized campus network will tend to interconnect sets of information resources with vastly different risk profiles. If students are housed on campus, public and even most private institutions will tend to view themselves as an ISP to their students--providing them basic Internet services in their homes. As such, students will tend to demand privacy and the same amount of freedom that they would expect from a home cable or DSL provider. In such a situation, risks to the institution may actually *i ncrease* if excessive security controls are applied to student networks. Contrast this with, for example, a campus's main HR system, and it stands to reason that information-security risk varies widely, both qualitatively and quantitatively.
It should therefore come as no surprise that the phrase "one size fits all" is frequently used pejoratively in IT. Attempting to place the same set of controls on vastly different information resources can be both perilous and costly, at least in the long term. Unfortunately, this is part of the problem with control-based

campuses that implement a variety of control-based mechanisms, indicates that data breaches have increased, even as controls have increased. More research is likely needed to provide more accurate metrics.

security, which, in its purest (and probably rarely extant) form, does not take risk into account, and therefore, cannot identify assets with different risk profiles.

The way risk-based security approaches deal with the vastly different risk profiles is to first identify them, and second, to attempt to *segment* the resources according to their risk profile. In the context of network-attached information resources, segmenting can be done at layer 1 (e.g. air-gaps or separate WDM lambdas for different risk-based networks) or layer 2 (e.g. separate VLANs). This is precisely where the Science DMZ comes in. Because the Science DMZ model prescribes segmentation to meet performance, troubleshooting, and security needs, it fits in nicely with a larger risk-based segmentation strategy. The Science DMZ can be viewed as the "LSDT segment" of a larger risk-based security-segmentation program.

Maintaining Reasonable Scope

For campuses deploying the Science DMZ who also use largely control-based approaches to security, a Science DMZ deployment can seem daunting. CISOs will want to sign off on the design and they may not like what they see as "missing controls." But it may seem even more daunting to try to use a Science DMZ deployment to change the way that the campus views security--in effect, a forcing-function pushing the campus from a largely control-based approach to a risk-based approach, just so some scientists can do data transfers! Even hybrid approaches will want to pay close attention to compensating controls.

It should not be a prerequisite that a major university's entire security strategy shift significantly just so a Science DMZ can be deployed. The good news is that the Science DMZ is only incompatible with control-based security in its purest form, and rarely do campuses actually practice such methods in their extreme. Because most campuses are capable of at least some level of risk-assessment, it is therefore important that the Science DMZ maintain a carefully-scoped risk profile, to ease the risk-assessment process. The resources located within the Science DMZ segment should *only* be geared toward maximizing the functionality *and security* of the LSDT function. Placing other information resources in the Science DMZ, such as email servers serving mailing lists, informational web servers that are not used for data transfers, etc., changes the risk profile and complicates security efforts. In order to maintain good segmentation by risk, the Science DMZ must remain narrow in scope.

Using the Science DMZ to Secure Research

The benefit of the Science DMZ is that, not only does it provide a method of balancing security and functionality for LSDT, but it does provide a way of securing *other parts of the campus network*. Consider the following example:

Research instruments are often managed by computers, and these computers run specialized software, albeit often on commodity hardware and using off-the-shelf operating systems. This often presents a "worst-of-both-worlds" security and risk profile: The custom software is rarely updated, patched, or even audited for security flaws, and the commodity operating system has known and commonly-exploited

vulnerabilities, but cannot be upgraded to a more secure version because of dependencies relating to the custom software.

This catch-22 gets worse when one considers that the custom system is often responsible for extracting raw data from the instrument. If that data has to be made available to collaborators or the public, the possibility of placing a dangerously insecure system on the public network now arises. This is the sort of headache that security officers often have to deal with, and the "solution" is often to throw a lot of controls at the system, and place heavy restrictions on it using stateful firewalls.

This raises two issues:

1. The controls may make the performance of the system so bad that data cannot be extracted at a reasonable rate.
2. Even so, the controls *m ay not be effective*, since wider access to at least certain resources on the system necessary to extract data may still expose vulnerabilities.

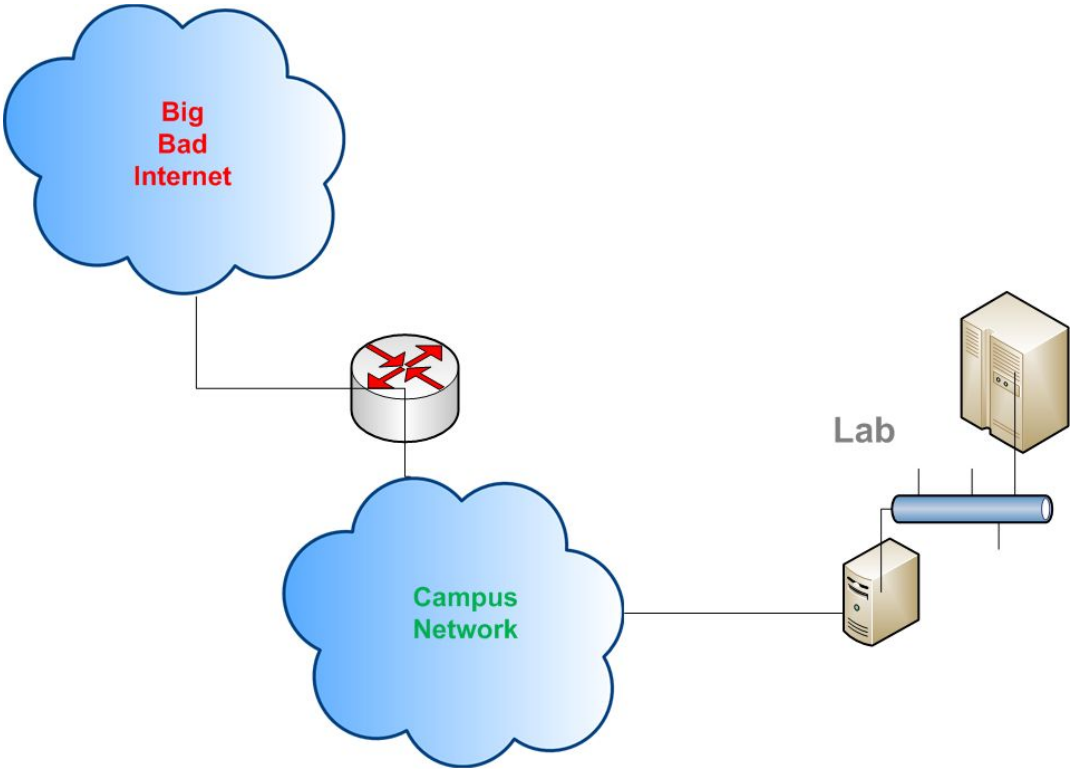


Figure 1: Pre-Science DMZ: I n this figure, the scientific instrument is on the far right, and its (potentially vulnerable) control system is connected to it, and to the main campus network, so that data from the instrument can be shared. The campus network must allow at least some access to the control system so that data-sharing requirements can be met. This raises security issues.

In this case, a Science DMZ solves both issues in an elegant and effective way. Rather than develop a one-off bastion host to access the data, a standard, supported, and scalable Science DMZ can support this particular research instrument, and possibly many other similarly-configured instruments. The Science DMZ can allow the instrument to be heavily walled-off from the rest of the world, and can only be

accessed by one or more data transfer nodes within the Science DMZ. For even more security, the instrument may be fully air-gapped on the network side, and the data may be transferred using a separate SAN system. In this model, the system driving the instrument mounts a LUN via fibre-channel and then unmounts it after the data is transferred. A DTN then mounts the LUN and transfers the data to outside collaborators. This is a somewhat stylized example, but it can be proven to work, and can provide a great deal of performance and security. Moreover, this model of segmentation that includes a Science DMZ, actually *reduces* risk and vulnerability, rather than adding risk.

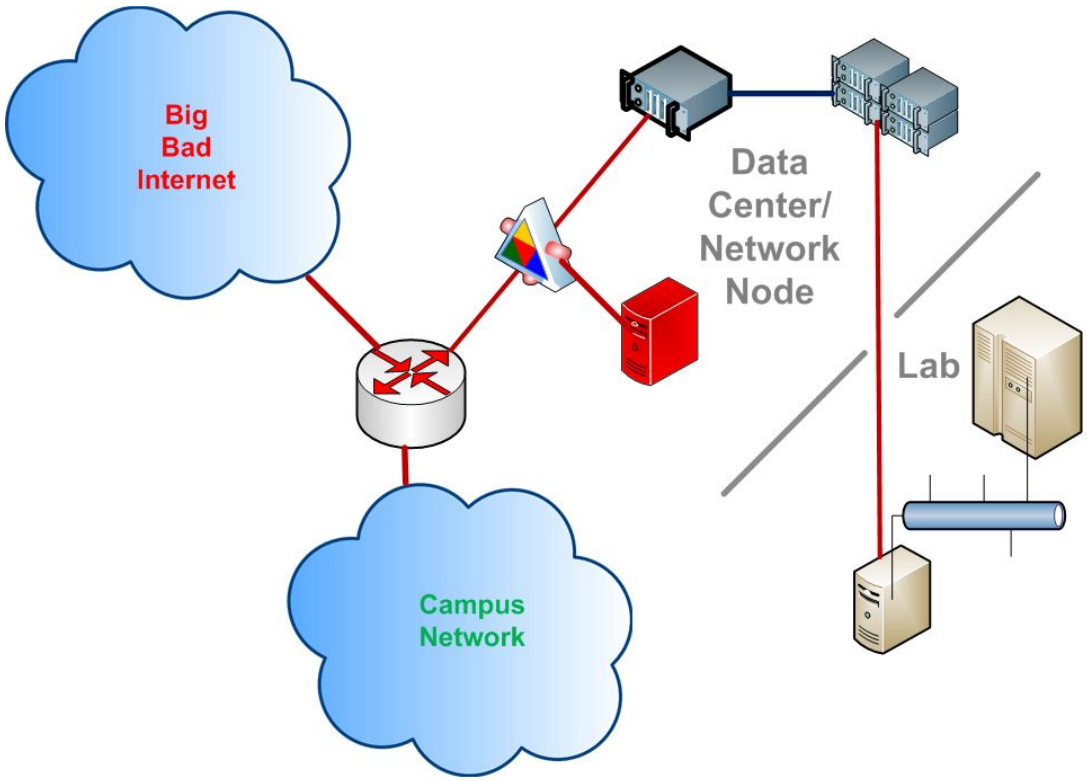


Figure 2: Post-Science DMZ: I n this scenario, a Science DMZ has been installed in the upper right, with a SAN-connected DTN (the grey boxes) and an optical tap and monitoring system (red computer). The control system is now disconnected from the main campus network and only mounts a LUN on the SAN in order to save data collected from the instrument. Once the data is saved, the DTN inside the Science DMZ mounts the LUN and allows the data to be exported over a high-performance WAN. The control system is protected, but data-sharing needs are still met.

Conclusion: The Science DMZ and the Flywheel Effect

Even where campuses practice a largely control-based security method, the example above shows how overall security can be improved for applications where data from research instruments must be shared over the network. As this is quickly becoming the norm in R & E, this kind of application is likely to exist on many campuses. Making use of the Science DMZ to provide high-performance data transfer capabilities, while carefully segmenting and managing risk, can actually allow for other parts of the campus network to be made *m ore secure*. By demonstrating success with risk-based segmentation, the Science DMZ can promote more instances of risk-based approaches to security. This can create a flywheel effect, where campuses eventually improve their posture at assessing and managing risk, and in the process, develop better methods and strategies that ultimately improve their overall security standing.

Security officers need to be made aware of the trade-offs inherent in various security architectures. In the case of the Science DMZ, security officers' concerns can be allayed by analyzing and documenting the risks that accrue to the Science DMZ itself, proposing and implementing compensating controls, and in demonstrating how the Science DMZ can substantially *improve* security on other parts of the campus network, as in the case above. As noted, controls on the Science DMZ itself are still necessary, but such controls can be demonstrated to match and mitigate the specific risks of the Science DMZ, when it is segmented away from the rest of the campus network.[8] By including these carefully-developed controls and firmly situating the Science DMZ architecture in a larger strategy of risk-based network security, campus information security can be substantially improved.

[8] Work is already being done on identifying sets of controls that are applicable to the Science DMZ's risk profile. See, for example, the work of Nick Buraglio and others, e.g. "Best Practices for Securing the Science DMZ, BroCon, 2014 (h ttps://www.youtube.com/watch?v=IPh3aZ18IuY) and "Securing the Science DMZ," Focused Technical Workshop, July 2014 (http://meetings.internet2.edu/media/medialibrary/2014/07/14/20140716-buraglio-sciencedmzsec.pdf).

Using Globus Auth to Streamline the Creation, Integration, and Use of Research Services

Ian Foster University of Chicago 5735 South Ellis Avenue Chicago, IL 60637 +1 (630) 252-4619 foster@uchicago.edu

Lee Liming University of Chicago 5735 South Ellis Avenue Chicago, IL 60637+1 (505) 899-4098 lliming@uchicago.edu

Steven Tuecke University of Chicago 5735 South Ellis Avenue Chicago, IL 60637+1 (630) 551-8711 tuecke@uchicago.edu

Abstract

Globus Auth is a foundational identity and access management platform service designed to address unique needs of the science and engineering community. It serves to broker authentication and authorization interactions between end-users, identity providers, resource servers (services), and clients (including web, mobile, and desktop applications, and other services). Globus Auth thus makes it easy, for example, for a researcher to authenticate with one credential, connect to a specific remote storage resource with another identity, and share data with colleagues based on their global identity. By eliminating friction associated with the frequent need for multiple accounts, identities, credentials, and groups when using distributed cyberinfrastructure, Globus Auth streamlines the creation, integration, and use of advanced research services. Here we introduce Globus Auth by describing how it can be used by a real research service, the Research Data Archive of the National Center for Atmospheric Research, to enhance both delivered capabilities and user experience.

1. Introduction

Progress in science and engineering is hindered by a pervasive lack of high-quality, easy-to-use applications and services. Small businesses have seen a transformational change in how information technology (IT) is delivered and used, slashing costs and increasing capabilities by outsourcing a wide range of business IT functions to software-as-a-service *business service providers* [9]. In principle, the data- and compute-intensive work of research laboratories could be similarly transformed, if various routine but resource-intensive operations (e.g., data management) could be outsourced to suitable *research service providers*. But in practice this transformation has not occurred.

Part of the problem is that research is a classic long tail market: different scientific communities, sub- communities, laboratories, and even individual researchers often have idiosyncratic information technology needs. But it is also the case that a lack of common infrastructure services makes it challenging to

develop new services, by introducing unnecessary *identity and integration friction*, as we now explain.

The developer of a new research service faces two major infrastructure challenges, namely (1) providing sophisticated identity and access management (IAM) functionality; and (2) integrating with multiple other services, that have been developed by independent parties, while providing a good user experience.

Addressing these challenges has been far too difficult for the vast majority of service providers. The result is a fragmented ecosystem of research services. For example, few scientific web applications and science gateways leverage federated identity systems such as InCommon [7]. Instead, each service provider cobbles together its own identity management solution. The result, all too often, is applications with limited functionality (due to the cost and expertise required to implement sophisticated IAM functionality), little integration (due to the difficulty in integrating different IAM approaches), increased cost to create and maintain (due to each group creating their own partial solutions), and poor user experience (due to inconsistent and incompatible IAM functionality)

Globus Auth [2] is platform as a service (PaaS) that addresses these challenges, with the goal of streamlining the creation, integration, and use of advanced research services [6]. In brief, it allows research service providers to outsource identity, credential, profile, and group management functions to a cloud-hosted, professionally managed service. In so doing, providers gain four major benefits. First, they gain access to sophisticated IAM functionality that would be

difficult for them to implement from scratch themselves. Second, they gain integration with other systems, based on standards such as OAuth2, OpenID Connect, SAML, and X.509. Third, they reduce implementation and operation costs: complex in-house code can be replaced with simple REST API calls to a professionally operated service. And fourth, they improve user experience by delivering high-quality, consistently presented IAM capabilities and interfaces.

In the rest of this article, we use a real-world example to illustrate how these benefits can be obtained in practice.

2. NCAR'S Research Data Archive

The National Center for Atmospheric Research (NCAR) maintains the Web-based Research Data Archive (RDA) [1], which contains more than 600 data collections. These collections, which range in size from gigabytes to tens of terabytes, include meteorological and oceanographic observations, operational and reanalysis model outputs, and remote sensing datasets to support atmospheric and geosciences research, along with ancillary datasets, such as topography/bathymetry, vegetation, and land use datasets. RDA users are primarily researchers at federal and academic research laboratories. In 2014 alone, more than 11,000 people downloaded more than 1.1 petabytes. Until recently, all downloads were over HTTP, either via Web browser, or via scripts that use wget or cURL.

HTTP downloads are known to be inefficient and unreliable over wide area, high speed networks. Use of scripts can mitigate these issues somewhat, but at the cost of increased complexity for users. In order to keep up with user demand for data and to provide its users with an easy to use, reliable, high performance delivery service, NCAR recently added the ability to download data via the Globus cloud-hosted data transfer service [4].

Globus provides simple web interfaces for setting up and monitoring downloads, and implements the downloads themselves by specialized software and protocols that usually outperform HTTP and that can continue a download even if the system being downloaded to (or from) is temporarily turned off or temporarily loses its network connection. The Globus transfer service thus ensure that downloads complete, regardless of how many times they are interrupted along the way [5].

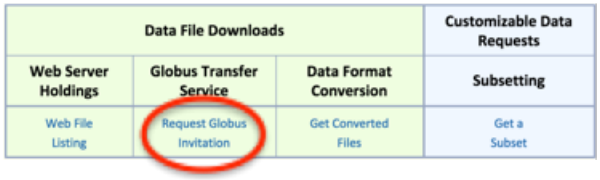


Figure 1: Example data access matrix from a dataset page on the RDA website. Selecting the highlighted link initiates a Globus data share for the dataset.

When NCAR added Globus data services to RDA, they leveraged several Globus features to integrate the RDA and Globus user experiences. When an RDA user is ready to download a batch of data from the RDA website, one of the options available via the website is, "Request a Globus Invitation" (see Figure 1). If the user selects that option, the RDA system automatically creates a folder on a Globus "shared endpoint" that contains the requested data, and uses Globus to invite the user to access this shared endpoint folder via the user's email address [8]. An email message is sent to the user with a link to the shared endpoint. By clicking on this link, the user can login to Globus, connect to the shared endpoint, and transfer the data wherever they need it: either to their
local system or to another national system, for example to perform further analysis on the data [8].

While the integration of RDA with Globus is quickly gaining popularity, it is unfortunately not as seamless as one would like. Its users must currently create a Globus identity (username and password) to access the data, instead of simply using the user's existing RDA identity. For the user to have single sign-on to both RDA and Globus, the user must link their RDA identity to their Globus identity (see Figure 2). The need to perform these tasks degrades the user experience and increases the complexity of the RDA-Globus integration.

In the following, we describe how RDA is using the new Globus Auth service to streamline its current integration with Globus capabilities—and also to add powerful new capabilities to RDA.

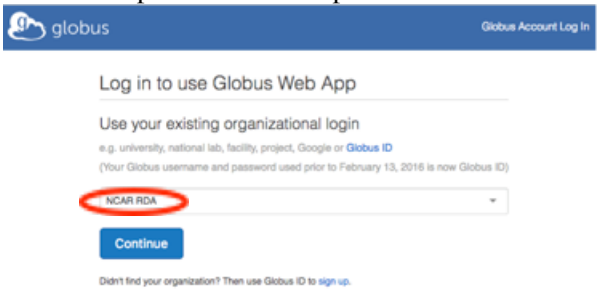


Figure 2: Globus support for NCAR RDA as an

identity provider (highlighted) means that users can use their RDA identity to authenticate to Globus services.

3. Improving RDA With Globus Auth

RDA can use Globus Auth to overcome identity and integration friction associated with its current implementation of IAM and Globus transfer capabilities, and thus to address the challenges described in the introduction. We use five examples to illustrate the opportunities.

3.1 Remove the Need for a Globus Identity

Globus Auth allows a Globus account to be created using any identity. Users no longer need to create a Globus username and password. Instead, since RDA is a Globus Auth-supported identity provider, Globus accounts can be created using any RDA identity. Since the Globus data transfer service uses Globus accounts provided by Globus Auth, an RDA user can then login to both RDA and the Globus transfer service using their RDA identity.

Globus Auth gives identity providers two options for such integration. First, it allows for identity provisioning by supported identity managers, via its REST API. RDA can use the Globus Auth REST API to proactively provision all RDA identities with Globus Auth. Second and alternatively, OpenID Connect [12] and SAML [11] identity providers (via CILogon) can configure Globus Auth to dynamically provision an identity with Globus Auth the first time it is used to login to Globus Auth.

Note that Globus Auth uses web-based federated identity protocols, such as OpenID Connect and SAML, to perform user login via its supported identity providers, so that Globus Auth is never required to see user passwords.

Depending on the configuration of a specific identity provider with Globus Auth, creation of a Globus account at first login with an identity can be made completely automatic. Alternatively, Globus Auth may prompt the user for additional Globus account information (e.g., email address, display name, and/or acceptance of Globus terms and conditions).

If an RDA user already has a Globus account using a different identity, Globus Auth makes it easy to link their RDA identity to this existing Globus account, rather than creating a new Globus account.

Globus Auth makes it easy for RDA to give its users single sign-on to RDA, as well as to other services that use Globus Auth, such as Globus data transfer.

3.2 IntegrateRDAandGlobusTransferAPI

RDA does not currently use the Globus data transfer REST API to manage transfers. Instead, RDA sets up a Globus shared endpoint with the appropriate data, and then directs the user to the Globus web application to transfer the data. The previous section describes how Globus Auth can enhance that experience by allowing web single sign-on to both RDA and Globus using the Globus identity.

However, Globus Auth allows RDA to go a step further, to integrate RDA directly with the Globus transfer service via the Globus transfer REST API. Thus, for example, the RDA web application could directly ask the user where (which Globus endpoint and path) they want their data sent. RDA would then act on the user's behalf to direct Globus to perform the transfer. So rather than the user leaving the RDA web application to perform transfers via Globus, RDA instead keeps the user in the RDA web application, and directs the Globus transfers behind the scenes on behalf of the user.

The mechanisms required to achieve this integration are straightforward. RDA must become an OAuth2 client [10] to Globus Auth. Then, when the user requests a transfer via the RDA web site, RDA performs a standard OAuth2 "authorization code grant" with Globus Auth to get an OAuth2 access token. RDA then uses this access token to request Globus transfers on the user's behalf via the Globus transfer REST API.

From the user's perspective, this new process is simple. They will be asked the first time this is done if they consent to this use of Globus transfer by RDA on their behalf. The user will not even be required to re-enter their password, assuming the RDA identity provider uses the standard web single sign-on technique of a session cookie to remember the user login. After the first transfer, in

which the user grants consent, all subsequent interactions between RDA and Globus will be transparent to the user.

3.3 LeverageOtherGlobus-enabledServices

Just as RDA integrates with the Globus transfer REST API, it could also integrate with other services, provided by Globus as well as third parties. We give two examples.

Globus provides a group management service that is integrated with Globus Auth and used by Globus transfer [6]. RDA could use this service in various ways: for example, to authorize access to restricted data sets by groups of users.

XSEDE services [13] such as the XSEDE User Portal (XUP) and XSEDE Resource Allocation Service (XRAS) will soon support Globus Auth access tokens in their REST APIs. Globus Auth can thus make integration of RDA with XSEDE resources and services as seamless as RDA's integration with Globus data transfer.

3.4 RemovetheNeedforanRDAIdentity

RDA currently requires that every user create an RDA username and password when they register with RDA. However, many RDA users already have accounts with federated identity providers, such as their universities (via InCommon) and Google.

Globus Auth makes it easy for RDA to add support for these federated identity providers. On its user registration page, RDA simply needs to add an option to create an RDA account to which the user can login using any identity provider supported by Globus Auth, instead of (or in addition to) requiring an RDA password. When this option is selected, RDA would simply act as a standard OpenID Connect client to Globus Auth. During user registration, and subsequently during user login, RDA would redirect the user's browser to Globus Auth, the user would login to their Globus account using their preferred identity (e.g., from their university, Google, etc.), and Globus Auth would redirect back to RDA. RDA can then get a standard OpenID Connect "id token" from Globus Auth that identifies the user.

Globus Auth takes care of all of the complexities of integrating with various identity providers via various protocols, linking multiple identities, etc. RDA can also get out of the business of managing passwords, helping users recover from lost passwords, etc., if desired.

3.5 Integration with RDA REST APIs

Just as RDA can seamlessly integrate with the Globus data transfer service, third party application and service developers may want to integrate with RDA. However, while RDA provides various REST APIs, these APIs currently require that the RDA username and password be passed with each request.

Once RDA integrates with Globus Auth in the manner described in the previous section, so that Globus accounts

to be used to login to RDA, it is a small step to also allow Globus Auth-issued access tokens to be used with the RDA REST APIs.

This approach has two major benefits to RDA. First, it allows clients to integrate with RDA as seamlessly as RDA integrates with Globus data transfer. Second, RDA can easily enhance its REST APIs with standard OAuth2 authorization, as used by the likes of Facebook, LinkedIn, Google, and Microsoft.

Globus Auth supports the use of a variety of authentication methods for acquiring access tokens, each suited to different purposes. For example: (1) OpenID Connect provides a standard Web federated identity protocol that is great for web and mobile application clients that want to integrate with RDA; (2) Globus Auth supports username and password authentication with some identity providers, which is useful for legacy applications that require username and password login; (3) Globus Auth will support X.509 client authentication, which is useful for integration from legacy grid systems; and (4) forthcoming support for app passwords will enable better command line application integration with RDA.

4. Conclusions

We have used the example of the NCAR Research Data Archive to illustrate how Globus Auth can be used to streamline the creation, integration, and use of advanced research services. In particular, we have described how RDA can easily leverage Globus Auth to provide enhanced IAM capabilities (e.g., authentication with campus credentials via InCommon), enhance integration with other science services (e.g., Globus transfer, XSEDE), and provide new capabilities (e.g., OAuth2 support in its REST APIs).

RDA's integration with Globus services is new, and Globus Auth has just recently become available to users. We look forward to working with NCAR to realize some of the new opportunities laid out in this article.

We hope it is clear that the methods that we presented here can easily be used by other research service providers to streamline their own services—and that the result will be an overall cyberinfrastructure ecosystem that is easier for researchers to use and that can more easily be applied to specific scientific challenges.

Acknowledgments

The development of Globus services has been supported in part by DOE DE-AC02-06CH11357; NSF ACI- 1053575 and ACI-1148484; NIH U24 GM104203 and 1- U54EB020406-01; the University of Chicago; a grant from the Sloan Foundation; and a grant of computer time from Amazon Web Services. Increasingly, operation of Globus services is financially supported by its subscribers [3].

References

1. CISL Research Data Archive. [Accessed March 1, 2015]; Available from: http://rda.ucar.edu.
2. Globus Auth API Specification. [Accessed July 1, 2015]; Available from: http://hdl.handle.net/11466/GlobusAuthAPISpecification.
3. Globus Provider Plans [Accessed July1, 2015]; Available from: https://www.globus.org/providers/provider-plans.
4. Transferring RDA data with Globus. [Accessed July 1, 2015]; Available from: http://ncarrda.blogspot.com/2015/06/transferring-rda-data- with-globus.html.
5. Allen, B., Bresnahan, J., Childers, L., Foster, I., Kandaswamy, G., Kettimuthu, R., Kordas, J., Link, M., Martin, S., Pickett, K. and Tuecke, S. Software as a Service for Data Scientists. *Communications of the ACM*, 55(2):81- 88, 2012.
6. Ananthakrishnan, R., Chard, K., Foster, I. and Tuecke, S. Globus Platform-as-a-Service for Collaborative Science Applications. *Concurrency - Practice and Experience*, 27(2):290-305, 2014.
7. Barnett, W., Welch, V., Walsh, A. and Stewart, C.A. A Roadmap for Using NSF Cyberinfrastructure with InCommon, http://hdl.handle.net/2022/13024, 2011.
8. Chard, K., Tuecke, S. and Foster, I. Efficient and Secure Transfer, Synchronization, and Sharing of Big Data. *Cloud Computing, IEEE*, 1(3):46-55, 2014.
9. Dubey, A. and Wagle, D. Delivering software as a service. *The McKinsey Quarterly*, May, 2007.
10. Hardt, D. The OAuth 2.0 Authorization Framework. Internet Engineering Task Force, Request for Comments: 6749, 2012.
11. Hughes, J. and Maler, E. Technical Overview of the OASIS Security Assertion Markup Language (SAML) v1.1, http://www.oasis-open.org/committees/security, 2004.
12. Sakimura, N., Bradley, J., Jones, M., Medeiros, B.d. and Mortimore, C. OpenID Connect Core 1.0 incorporating errata set 1. 2014; Available from: http://openid.net/specs/openid-connect-core-1_0.html.
13. Towns, J., Cockerill, T., Dahan, M., Foster, I., Gaither, K., Grimshaw, A., Hazlewood, V., Lathrop, S., Lifka, D., Peterson, G.D., Roskies, R., Scott, J.R. and Wilkins-Diehr, N. XSEDE: Accelerating scientific discovery. *Computing in Science and Engineering*, 16(5):62-74, 2014.