CTSC
CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

2016 NSF Community Cybersecurity Benchmarking Survey Report

28 April 2017

For Public Distribution

Robert Cowles, Craig Jackson[1]

[1] Project Lead and Co-PI, scjackso@indiana.edu

About the NSF Cybersecurity Center of Excellence

Our mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

Acknowledgments

The authors thank Amy Starzynski Coddens, Jim Marsteller, and Jeannette Dopheide who participated in the development and socialization of the survey, as well as Mark Krenz and other team and community members who contributed ideas to the content of the survey.

Many thanks to all the respondents.

This document is a product of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). CTSC is supported by the National Science Foundation under Grants Number ACI-1547272. For more information about the Center for Trustworthy Scientific Cyberinfrastructure please visit: https://trustedci.org/. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Using & Citing this Work

This work is available on the web at the following URL:
http://hdl.handle.net/2022/21355

Table of Contents

Executive Summary

Benchmarking information is frequently used to develop a common sense of cybersecurity's status and norms within a community. The purpose of this survey project was to collect, analyze, and publish useful baseline benchmarking information about the NSF science community's cybersecurity programs, practices, challenges, and concerns. We received 27 responses to the survey including 16 responses from respondents with annual budgets greater than $1M (including 9 responses from the ~25 NSF Large Facilities). Highlight results and findings include the following:

- Cybersecurity budgets vary widely for respondents with annual budgets above $1M, with Large Facilities ranging from 0.02% - 1.5% of annual budget and big projects ranging from 0.25% - 4.58% of annual budget. Possible explanations for this variation include, but are not limited to: (a) budget sizes are driven by facility or project mission rather than adhering to some budgetary rule of thumb and/or (b) leadership for these large awards have highly varied beliefs regarding the need for cybersecurity investment. Average cybersecurity budget as a percentage of IT budget sits at the low end of the average values found in industry.
- Few projects with annual funding below $1M have a cybersecurity budget (2 of 10), or implement programmatic safeguards (1 of 10) or significant numbers of operational safeguards (2 of 10) on their own.
- Nearly all (24) respondents undertake some cybersecurity policy development. However, several respondents, including 3 of 16 with >$1m dollar budgets, do not employ a framework or identified guidance resource to help shape the cybersecurity program.
- Many projects, including some who have adopted a framework, do not have process for accepting residual information security risk. Nearly half of the respondents in each category selected "There is no explicit risk acceptance process" (Large Facility - 5 of 9, Big - 3 of 7, Small - 5 of 9).
- Few respondents produce inventories of critical systems (9) or use data classification scheme (8). Only 5 of 9 responding Large Facilities employ inventories.
- Only 6 respondents utilize multi-factor authentication.
- Most respondents with annual budgets above $1M detected cybersecurity incidents in past year (Large Facilities - 7 of 9, Big - 4 of 7). Only respondents with a significant number of operational safeguards detected cybersecurity incidents.
- Respondents reported a range of negative impacts associated with the incidents they detected [Q19], including loss of reputation, decreased confidence in data integrity, temporary or permanent inability to collect or analyze data, interruption of remote access (4), significant cost of incident recovery procedures, cost of additional remediation procedures / controls (2).
- However, many respondents reported "Does not apply" regarding the types of impact of cybersecurity incidents (LF - 3 of 8, Big - 4 of 6, Small - 10 of 10).
- Large Facility respondents indicate a greater concern than respondents in the other categories for threats of sabotage or other events affecting availability of critical systems (LF - 6 of 9, Big - 2 of 7, Small - 2 of 10). Other categories of respondents most commonly indicated concern about modification of data (LF - 3 of 9, Big - 4 of 7, Small - 4 of 10) or unauthorized access to systems or networks (LF - 2 of 9, Big - 4 of 7, Small - 4 of 10).
- Patching interval for moderate and low vulnerabilities often (13 of 22) exceeds one month.
- All 26 respondents reported that they develop software in house.

1 Introduction

Benchmarking information is frequently used in the cybersecurity field to develop a common sense of status and norms within a community or sector. At the 2015 NSF Cybersecurity Summit, an informal query of the community members indicated the NSF science community would respond to such a survey and utilize the results.

The purpose of CTSC's survey project was to collect, analyze, and publish useful baseline benchmarking information about the NSF science community's cybersecurity programs, practices, challenges, and concerns.

In this report, we describe our methodology for constructing the survey and collecting responses (Section 2), overview the survey results (Section 3), and offer an analysis of those results (Section 4). In Section 5, we conclude with some reflection and next steps.

2 Methodology

In this section, we describe our target respondent community, target audience for this report, survey construction, and response collection.

2.1 Responding Community and Audience

2.1.1 NSF Project Community

NSF awards approximately 9,000 grants and cooperative agreements each year; there are approximately 30,000 active awards at the current time.[2] Among those active awards are ~25 NSF Large Facilities[3]. This survey was targeted to the entire NSF community of science projects and facilities.

2.1.2 Audience for This Report

We envision a number of groups as the audience for this report.

- CTSC. The survey results will assist CTSC in tailoring its services to the current state of cybersecurity at NSF-funded facilities and projects.
- NSF-funded science projects and facilities. The survey results may assist science projects and facilities in developing a sense of norms and practices in the community.

[2] https://www.nsf.gov/awardsearch/advancedSearch.jsp Accessed 27 April 2017.
[3] https://www.nsf.gov/bfa/lfo/docs/large-facilities-list.pdf

- NSF leadership and program officers. The survey results may give NSF leadership and program officers greater insight into norms and practices in the community.

2.2 Survey Construction

We designed survey questions to collect information on respondents' budgets and other descriptive attributes relevant to cybersecurity, as well as information regarding specific cybersecurity practices, events, and concerns. A text copy of the survey is included as Appendix A.

We expected the size of the total annual budget along with the IT and cybersecurity budgets (if any) to give a rough indication of the resources potentially available to invest in cybersecurity. We expected the diversity of the user population (users from how many external sites) along with software development to be indicators of the complexity of the cybersecurity environment. We included questions if there is an identified CISO and/or cybersecurity group. We included questions about baseline cybersecurity practices and controls including: policy development; risk acceptance; external requirements; identity management; programmatic controls; operational controls; patch frequency; and cybersecurity incident frequency and impact. In the final section, we asked what would help the most in improving the cybersecurity program and the threats of greatest concern.

In late June, 2016, we sent an email to CTSC's cybersecurity discussion list requesting input from the community concerning questions they would like to appear on the survey.

> CTSC is developing a benchmarking survey to collect and aggregate information about cybersecurity in the NSF science community. We anticipate including questions on topics like cybersecurity budgets, type and frequency of security incidents, and most-used best practices resources and frameworks.
>
> We want to ensure the survey report is of maximum utility to the NSF researchers, projects, and facilities, and encourage a high level of participation. Your input will help us meet that goal.

Three responses were received and resulted in two additional questions in the survey.[4]

Response to this survey was voluntary and optional. To encourage a higher response rate and more complete responses, we purposely avoided collecting project identifying information (e.g., project name, award number). The survey announcement (above) stated, "Please note that we

[4] See, Q16 and Q17 in Appendix A

are aggregating responses and minimizing the amount of project-identifying information we're collecting. CTSC will release results that we believe provide anonymity to the individual project or facility respondents."

2.3 Response Collection

The survey was announced August 15, 2016 on CTSC's Announce email list (almost 500 subscribers at the time):

> Dear colleagues at NSF facilities and projects,
>
> Please complete the 2016 NSF Community Cybersecurity Benchmarking Survey. The goal of the survey is to collect and aggregate information about the state of cybersecurity for NSF projects and facilities, and produce a report that will help the community level set and give other stakeholders (like CTSC!) a richer understanding of the environment and how to help. We want to ensure the survey report is of maximum utility to the NSF researchers, projects, and facilities, and encourage a high level of participation. Your responses will help us meet that goal. Please note that we are aggregating responses and minimizing the amount of project-identifying information we're collecting. CTSC will release results that we believe provide anonymity to the individual project or facility respondents.
>
> https://docs.google.com/forms/d/e/1FAIpQLSeqOFdYMPTAv5WMXS_Mduu1vlwdWbzW7KZPcxykQaSCZEx6tg/viewform
>
> Each NSF project or facility should submit only a single response to this survey. Completing the survey may require input from from the PI, the IT manager, and/or the person responsible for cybersecurity (if those separate areas of responsibility exist). While answering specific questions is optional, we strongly encourage you to take the time to respond as completely and accurately as possible. If you prefer not to respond or are unable to answer a question for some reason, we ask that you make that explicit (e.g., by using "other:" inputs) and provide your reason.
>
> The response period closes October 14, 2016.
>
> Thank you,
>
> Craig Jackson, Jim Marsteller, Amy Starzynski-Coddens, and Bob Cowles
> CTSC

At the NSF Cybersecurity Summit on August 17, 2016, the survey was highlighted during a talk in a plenary session. Reminders were posted to the Announce email list on September 14 and October 4, and Jim Marsteller mentioned the survey during the FacSec meeting in September. On October 18, the deadline for responding to the survey was extended until October 28.

3 Results

See Appendix B for tables detailing the results from the survey. Note that some questions were not answered by all respondents; some questions allowed multiple selections as a response; and some questions allowed no more than two selections.

Below, we provide a high level picture of the response rates and the categories of respondents that emerged in this response group.

3.1 Response Rates

The survey received 27 responses. In light of the thousands of active NSF awards, we caution against any conclusion that these results are representative of the community at large. However, we received a respectable 9 responses from ~25 Large Facilities, plus 7 additional responses from the awards with annual budgets greater than $1,000,000.

3.2 Response Categorization

For the purpose of our analysis, we divided the responses into three groups: LF, Big, and Small. In developing the survey, we expected multiple variables would significant roles in how we would end up grouping the respondents. However, after looking closely at the data, annual budget alone was most helpful in grouping the respondents into meaningful categories for analysis. Nine of the respondents identified themselves as representing Large Facilities; all have large, multi-million dollar annual budgets and significant, long-term capital-intensive programs. They comprised the "LF" category. For the 18 responses from non-Large Facility[5] respondents, we included the larger projects or facilities (annual budget greater than $1M) in a "Big" category (7 respondents), and the respondents with a smaller total budget (annual budget less than $1M) in the "Small" category (10 respondents). This choice of dividing line coincided with a break in the reported annual budgets between $2M and $400K. At times, the responses from the LF category and the Big category were similar enough that we refer to the combination as the "LF+Big category".

[5] One of the 18 responses did not contain sufficient information to categorize, so was not included in the analysis.

4 Analysis

In this section, we highlight results we found interesting, surprising, encouraging, or concerning. Frequently, we utilize the respondent categories (see, Section 3.2) to describe the results. The numbers in square brackets (e.g., [Q6]) refer to the relevant survey question (see Appendix A).

We took the responses at face value, even when they seemed strange, inconsistent, or improperly formatted. The only exception is one response we were unable to categorize. Also, we used only non-null/non-zero responses in calculating average; including null/zero responses in the budget averages would so heavily skew the results as to render the averages meaningless.

4.1 Project or Facility Budget

Respondents were asked to provide the annual budget [Q1], the annual IT budget [Q2], and the annual cybersecurity budget [Q3] for their project or facility. There were more than three orders of magnitude variation in the annual budgets reported. Based on the variance in mission from large multi-year data-gathering instruments to smaller grants funding less than a researcher for a year, we were not surprised to see wide variation in the percentages of the annual budget devoted to IT and cybersecurity. Accounting practices (e.g., whether labor costs are included in the budget categories) may also have played a large role in the variability.

	LF category	Big category
Cybersecurity as % of Annual Budget (median value)	0.3%	0.4%
Cybersecurity as % of Annual Budget (range)	0.02% - 1.5%	0.25% - 4.58%
Cybersecurity as % of IT Budget (median value)	3% - 5%	1.25% - 5%
Cybersecurity as % of IT Budget (range)	0.43% - 12%	0.35% - 21.25%

Using median values, the LF and the Big categories were very similar both for cybersecurity budget as a percentage of total annual budget and as a percentage of the IT budget, and sit at the low end of the average values found in industry.[6] However, these median values mask a

[6] Russell, S., Jackson, C. and Cowles, B., “Cybersecurity Budgeting”, Presented at the 2016 Cybersecurity Summit for Large Facilities and Cyberinfrastructure, Alexandria, Virginia, August, 2016, accessed April 27, 2017,

wide variation in each of the categories. Possible explanations for this variation include, but are not limited to: (a) budget sizes were driven by facility or project mission rather than adhering to some budgetary rule of thumb and/or (b) leadership for these large awards had highly varied beliefs regarding the need for cybersecurity investment.

For Small category respondents, the reported IT budget was zero for 6 of 10 respondents and cybersecurity budget was zero for 8 of 10 respondents. At the funding level for the Small category, this zero response for budget may have reflected that IT and cybersecurity were either not separate budget items or the respondents depended on the host institution for cybersecurity. Because only two respondents in the Small category listed both an IT budget and a cybersecurity budget, the Small category is not included in the table above.

4.2 Project or Facility Attributes

Survey questions in this group were meant to uncover information about the environment in which cybersecurity takes places.

4.2.1 Respondents in the LF+Big category had complex authentication environments with 15 of 16 accommodating users from multiple external institutions [Q5] and many indicated more than 3 external institutions are involved (12 of 15). These responses are consistent with the fact that larger budget projects depend on collaboration from multiple institutions.

4.2.2 Relatively few respondents in the Small category (4 of 9) had external users. Even so, we were surprised at the number of respondents in the Small category with external users. Indicative of the more complex environment, even with a small annual project budget, most of these respondents listed an explicit IT budget (3 of 4) and half listed an explicit cybersecurity budget (2 of 4).

4.2.3 A majority of respondents in the LF+Big category had a specific role (e.g., ISO - Information Security Officer) [Q6] with cybersecurity responsibilities (12 of 16) and/or an identified cybersecurity group (12 of 16), usually within IT (11 or 16). Very few had neither a person nor a group for cybersecurity [Q7] (LF - 1 of 9, Big - 2 of 7). We were surprised and concerned that any of the LF category respondents did not have at least a part-time person with a cybersecurity role (2 of 9).

https://hdl.handle.net/2022/21161 pp. 102-109. According to most surveys, cybersecurity budgets were in the range of 3% to 12% of the IT budget.

4.2.4 None of the respondents in the Small category (0 of 10) had an identified individual role for cybersecurity responsibility [Q6]; however, a few (3 of 10) do had an identified cybersecurity group [Q7] . All three in the Small category with an identified cybersecurity group also listed an explicit IT budget and had external users.

4.2.5 All respondents indicated they perform software development and use a software repository (26 of 26) [Q8]. The LF+Big category respondents all used compiled languages (16 of 16), and almost all used interpreted languages (13 of 16). In the Small category, half of the respondents used only one or the other type of language (Interpreted - 8 of 10, compiled - 7 of 10, both - 5 of 10). Most respondents in the LF+Big category performed issue tracking/vulnerability management for the developed software (15 of 16), but only half of the Small category did so (5 of 10). Code signing (LF+Big - 5 of 16; Small -1 of 10) was infrequent. We were surprised by the ubiquity of software development. In the Small category of respondents, there was a close match for issue tracking/vulnerability management with continuous integration (5 of 5), automated testing (4 of 5), and use of both language types (4 of 5). It was also somewhat surprising that, for the respondents in the LF+Big category, code signing (5 of 15) and static and/or dynamic analysis (6 of 15) were not more common, although some form of automated testing was frequently listed (12 of 16).

4.3 Cybersecurity Program and Practices

4.3.1 Almost all respondents undertake some form of policy development (24 of 26). In the LF+Big category, cybersecurity policy development and acceptance [Q9] tended to be performed by a cybersecurity or IT person (LF - 7 of 9, Big - 5 of 7) with project leadership also playing a role in the Big category (6 of 7). In the Small category, project leadership (4 of 10) or the host institution (3 of 10) were listed by respondents. There were some Small category responses selecting both project leadership AND selecting “no process” (3 of 10) leading us to suspect that, while there was responsibility for policy development, there was no formal policy adoption process.

4.3.2 Almost all of the respondents in the LF+Big category utilized some form of framework or guidance (LF - 8 of 9, Big - 5 of 7) [Q10] for their cybersecurity program; almost none of the respondents in the Small category used any guidance documents (1 of 10). We were surprised to learn that projects with large budgets were not using a framework or guidance and were concerned that guidance was so rarely used by the Small category projects.

4.3.3 For acceptance of residual risk [Q11], nearly half of the respondents in each category selected “There is no explicit risk acceptance process” (LF - 5 of 9, Big - 3 of 7, Small - 5 of 9) and most of the other responses were “Senior managers or PI” (LF - 3, Big - 3, Small - 2). For the respondents in the LF+Big category who responded that there was no process, all but one claimed to be using a cybersecurity framework (7 of 8). The process of residual risk acceptance is a central mechanism of any risk-based approach to cybersecurity and is vital for communicating to process/service owners and leadership. Any complete framework will include risk acceptance, so it is very surprising to see respondents that claimed to be following a framework (*e.g.*, NIST RMF) and yet did not have a process for accepting residual risk. Possible explanations for these results include, but are not limited to, partial or immature utilization of risk-based approaches to cybersecurity.

4.3.4 Large Facilities are bound by the external information security requirements [Q12] spelled out in their cooperative agreements and most (8 of 9) respondents in that category responded accordingly. Personally Identifiable Information (PII) protection requirements affected 20-30% of the respondents (LF - 3 of 9, Big - 2 of 7, Small - 2 of 10). A few respondents reported non-disclosure agreements (LF - 3 of 9, Big 1 of 7).

4.3.5 Most LF+Big category respondents relied on a project or facility issued userid/password for identity management [Q13] (LF+Big - 12 of 16, Small - 4 of 10) and the Small category respondents tended to rely more on credentials from the host institution (LF+Big - 4 of 16, Small - 6 of 10). Almost half of the respondents indicated they also use project or federated certificates (LF+Big - 7 of 16, Small - 4 of 10).

4.3.6 For programmatic safeguards[7] [Q14], the most common selections for LF category respondents were overarching strategy (7 of 9), documented standards/baselines (7 of 9), conduct risk assessments (7 of 9), incident response plan (8 of 9), and disaster recovery plan (7 of 9). For respondents in the Big category, only overarching strategy, documented standards/baselines, and disaster recovery plan managed to obtain more than a majority (4 of 7). We were very concerned that the inventory of critical assets (5 of 9) and data classification (5 of 9) were not more prevalent for Large Facilities. Actually, this low number for an inventory of critical systems (10 of 26) or a data classification scheme (9 of 26) across all categories of respondents is troubling. These are foundational, baseline controls and are emphasized in most

[7] For the purposes of this survey, “programmatic safeguards” are primarily composed of administrative, management and policy cybersecurity activities as distinct from “operational safeguards” that are more technical in nature. We distinguish the safeguards since different skill-sets are often required for implementation, and to break up the questions capturing safeguards/controls.

if not all of the available cybersecurity frameworks and control sets.[8] [9] All projects, from the largest to the smallest, need to know what data are important to protect and the systems used to store and process that data.

In the Small category, except for one respondent with a significant cybersecurity budget and many external users, no programmatic safeguards were selected except for one other respondent selecting training. A possible explanation for this response pattern is strong reliance on the host institutions' safeguards.

4.3.7 The respondents in the LF+Big category typically had many operational safeguards [Q15]; the most commonly selected controls were firewalls (14 of 16), physical controls (13 of 16), and centralized logging (14 of 16). Respondents in the LF category, in particular, also commonly selected antivirus (8 of 9), vulnerability management (7 of 9), intrusion detection/prevention systems (7 of 9), and scanned for vulnerabilities or configuration errors (7 of 9). The Small category had a very sparse set of controls and, again, the reasonable conclusion is that they depend on the host institution for operational safeguards. However, one Small respondent that had users from many external sites had also implemented most of the operational controls. Few respondents in any category indicated that multi-factor authentication (MFA) (LF - 2 of 9, Big - 3 of 7, Small - 1 of 10) or data loss prevention/encryption (LF - 3 of 9, Big - 3 of 7, Small - 2 of 10) had been implemented. We note that MFA is a game-changing control and is increasingly seen as a critical security control, particularly with respect to accounts with privileged access or access to sensitive information. Only a few respondents subject to external requirements for PII or Protected Health Information (PHI) protection had also deployed encryption/data loss prevention (3 of 7). Even more scarce were respondents performing tabletop exercises (LF - 3 of 9, Big - 1 of 7, Small - 0 of 10), and penetration testing (LF - 3 of 9, Big - 2 of 7, Small - 0 of 10).

4.3.8 Many LF+Big category respondents patched critical vulnerabilities [Q16] in two days or less (LF - 5 of 8, Big - 5 of 7), and the remainder patched them within a week. For the Small category, <2 day patching of critical vulnerabilities was not as prevalent (2 of 7) compared with 1 week patching (5 of 7). Generally speaking, important vulnerabilities are patched within a week (LF - 8 of 9, Big - 5 of 7, Small - 4 of 6) and moderate vulnerabilities are patched within a month (LF - 9 of 9, Big 4 of 6, Small - 3 of 6). Most LF category respondents indicate patching low vulnerabilities within a month (6 of 8); however, a number of the categories indicated the patching interval is longer than a month for moderate (Big - 2 of 6, Small - 3 of 6), and for low

[8] See, the CIS Critical Security Controls for Effective Cyber Defense, specifically CSC 1 and CSC 2.

[9] https://www.asd.gov.au/publications/protect/Essential_Eight_Explained.pdf The first implementation step is to determine which assets require protection.

vulnerabilities (LF - 2 of 8, Big - 7 of 7, Small - 4 of 7). This length of time is concerning because privilege escalation vulnerabilities are often categorized as low[10], but they are used in an attack chain of advanced exploit scenarios.[11]

4.3.9 The respondents in the LF+Big category were split on management of cloud accounts [Q17] between having the accounts integrated (LF - 3 of 7, Big - 2 of 4) or having separate accounts (LF - 4 of 7, Big - 2 of 4). In the Small category, respondents indicated that separate accounts are used (8 of 8).

4.3.10 Most respondents in the LF category and a majority of the Big category respondents detected cybersecurity incidents in past year [Q18] (LF - 7 of 9, Big - 4 of 7). Only one in the Small category detected a cybersecurity incident (1 of 9). Only respondents with a significant number of operational safeguards are detecting cybersecurity incidents. The low number of cybersecurity incidents detected is either remarkable or a cause for concern (i.e., concern that the detection capabilities are too weak to detect the intrusions that are actually occurring).

4.3.11 Respondents reported a range of negative impacts associated with the incidents they detected [Q19], including loss of reputation, decreased confidence in data integrity, temporary or permanent inability to collect or analyze data, interruption of remote access (4), significant cost of incident recovery procedures, cost of additional remediation procedures / controls (2), as well as the following written in by respondents: “individual workstation,” “false alarm,” and “suspend accounts.” However, many respondents reported “Does not apply” regarding the types of impact of cybersecurity incidents (LF - 3 of 8, Big - 4 of 6, Small - 10 of 10).

4.3.12 For those LF+Big category respondents reporting an incident in the past year, the most commonly cited as having the greatest impact [Q20] were compromised workstation(s) (5 of 9), and compromised servers (2 of 9).

4.4 Cybersecurity Concerns

4.4.1 About half of the respondents in all categories selected more budget and/or more staff for the best way to improve their cybersecurity program [Q21] (LF - 4 of 9, Big - 4 of 7, Small - 5 of 10). One-third of the LF category respondents indicated a cybersecurity steering committee would produce the most improvement (3 of 9). Half of the respondents in the LF+Big category

[10] https://isc.sans.edu/forums/diary/Privilege+escalation+why+should+I+care/15863/
[11] https://blog.varonis.com/the-cyber-kill-chain-or-how-i-learned-to-stop-worrying-and-love-data-breaches/

selected options that may be indicative of governance issues (steering committee, reward/discipline systems, senior management commitment) (9 of 16).

4.4.2 For threats that were most concerning [Q22], respondents for the LF category indicated a higher concern than respondents in the other categories for threats of sabotage or other events affecting availability of critical systems (LF - 6 of 9, Big - 2 of 7, Small - 2 of 10). Other categories of respondents more commonly indicated concern with modification of data (LF - 3 of 9, Big - 4 of 7, Small - 4 of 10) or unauthorized access to systems or networks (LF - 2 of 9, Big - 4 of 7, Small - 4 of 10). This distribution of responses matches our assumption that Large Facilities are likely to have valuable instruments producing large amounts of data for which availability is extremely important. Interestingly, of the 7 respondents indicating they were subject to rules concerning PII or PHI, only one listed loss of confidential data as one of the most concerning threats.

5 Conclusion

Though we received far too few responses to claim a representative sample of the NSF community as a whole, the responses at least suggest a number of interesting, and sometimes concerning, facts about the state of cybersecurity in the NSF science community. Particularly for Large Facilities and projects with larger budgets, we hope these results and analysis provide some benchmarking insight and inspire discussion.

Looking ahead, CTSC will use this report to fuel discussions and inform its services. Moreover, we will look for community feedback on whether to conduct a survey in 2017 and, if so, how to improve it.

We are unsure what to take away from the low response rate. Voluntary surveys are not known for particularly high response rates, and this one certainly required some time and effort to complete. We'll be looking to the community to determine if the 2016 survey was a useful as a one-time peek into cybersecurity at the community level, a first step in tracking our progress, or otherwise.

Having administered the survey once, we have identified a few areas for improvement:

- It is likely to be the case, especially for the Small category, that safeguards are provided by the host institution and not missing as the current data might suggest. In subsequent surveys, it would be important to capture that information but it might be difficult or awkward to implement in the Google survey framework.

- In future surveys, we may be able to better clarify whether labor costs (fully burdened) are included in the IT and cybersecurity budget values. Also whether cybersecurity includes IT operational activities like vulnerability scanning, configuration management, and patching.
- The ubiquity of software development suggests there may be additional questions to include.

Appendix A: Survey

NSF Community Cybersecurity Benchmarking Survey

Instructions for completing survey

An NSF project or facility should submit only a single response to this survey. Completing the survey may require input from from the PI, the IT manager, and/or the person responsible for cybersecurity (if those separate areas of responsibility exist). While answering specific questions is optional, we strongly encourage you to take the time to respond as completely and accurately as possible. If you prefer not to respond or are unable to answer a question for some reason, we ask that you make that explicit (e.g., by using "other:" inputs) and provide your reason. CTSC will release results that we believe provide anonymity to the individual project or facility respondents.

Project or Facility Budget

If you are unable to answer, please provide a reason in the space provided

1. What is your project or facility's annual budget?

Estimate to 1 or 2 significant digits, e.g., $3M, $500K, $23,000

2. What is your project or facility's annual information technology budget?

Estimate to 1 or 2 significant digits, e.g., $1M, $50K, $23,000

3. What is your project or facility's annual cybersecurity budget?

Estimate to 1 or 2 significant digits, e.g., $0.1M, $50K, $23,000

Project or Facility Attributes

4. Is your project or facility an NSF Large Facility?

List of Large Facilities -- https://www.nsf.gov/bfa/lfo/docs/LargeFacilitiesListFeb2016.pdf

Mark only one oval.

- Yes
- No
- Don't know

5. Do individuals from multiple institutions authenticate to the resources of your project or facility?

Mark only one oval.

- Yes - 2 or 3 institutions
- Yes - more than 3 institutions
- No
- Don't know

6. Does your project or facility have a person with defined authority for developing and maintaining a cybersecurity program (e.g., ISO, CSO, CISO)?

Mark only one oval.

- Yes, full-time
- Yes, part-time
- No
- Don't know

7. Is there an identifiable group devoted to cybersecurity within your project or facility?

Mark only one oval.

- Yes, part of IT
- Yes, and separate from IT
- No
- Don't Know

8. Does your project or facility develop or maintain software? If so, what policies, processes or tools do you use?

Check all that apply

- Coding standards
- Interpreted languages (e.g., PHP, Python, Ruby, Perl)
- Compiled languages (e.g., C, C++, Rust, Java)
- Source code repositories
- Automated testing
- Continuous Integration
- Static and/or dynamic analysis
- Issue tracking / vulnerability management
- Testing policy (e.g., regression testing of patches)
- Code signing
- Automated documentation tools (e.g., pydoc)
- Not applicable
- Other:

Cybersecurity Program

9. How are cybersecurity policies developed and officially adopted within your project or facility?

Check all that apply

- IT Manager or cybersecurity person is responsible
- A formal governance board or group has been established to authorize the policies
- PI or other project or facility leadership are responsible
- There is no formal authorization or adoption process
- The host institution(s) provide the policies
- Other:

10. What framework or guidance (if any) has your project or facility adopted for how cybersecurity is done?

Check all that apply

- CIS Critical Security Controls (a. k. a. SANS Top 20) - https://www.sans.org/critical-security- controls
- NIST Risk Management Framework - http://csrc.nist.gov/groups/SMA/fisma/framework.html
- ISO (ISO/IEC 27005)

- CTSC's Guide - http://trustedci.org/guide/
- None
- Other:

11. Who accepts residual cybersecurity risk (i. e., the remaining risk after reasonable cybersecurity controls are established)?

Check all that apply

- A cybersecurity person
- IT manager
- System or process owner
- Senior managers or PI
- There is no explicit risk acceptance process
- Other:

12. What external cybersecurity requirements (if any) are imposed on your project or facility?

Check all that apply

- State or federally mandated protection of PII
- Protected health information
- Non-disclosure or contractual agreements
- Classified information - https://en.wikipedia.org/wiki/Classified_information_in_the_United_States
- FISMA
- Cooperative agreement terms
- None
- Don't know
- Other:

13. What kind(s) of identity management does your project or facility employ to control access to its resources?

Check all that apply

- The parent institution's identity management
- Separately maintained project or facility userid/password
- Independent project or facility certificate-based infrastructure
- Federated identity management technology
- Other:

14. What programmatic cybersecurity safeguards has your project or facility implemented?

Check all that apply

- Utilize cybersecurity maturity model to assess and/or plan program evolution
- Have an overarching cybersecuriy strategy, policy or plan
- Have documented cybersecurity standards/baselines for employees and/or external researchers
- Conduct risk assessments
- Inventory critical information assets
- Monitor/analyze security intelligence
- Have a cyber incident response plan

- Have a roadmap for cybersecurity improvements
- Have a data classification scheme
- Require periodic cybersecurity awareness training for personnel
- Have business continuity/disaster resovery plans
- Have an Information Security governance structure
- Review by external organizations
- None
- Other:

15. What operational cybersecurity safeguards has your project or facility implemented?

Check all that apply Check all that apply.

- Multi-Factor Authentication
- Centralized logging system
- Data loss prevention / file encryption
- Vulnerability management
- Intrusion Detection Systems / IPS
- Anti-virus / Anti-spam / spyware / phishing solutions
- Real-time alerting of possible attacks / anomalies
- Physical access controls to critical resources
- Network firewalls that block all but required access ports / protocols
- Scan for vulnerabilities or configuration errors
- Internal tabletop exercises to gauge organizational response
- Penetration or phishing tests
- None
- Other:

16. How frequently are patches applied based on the severity rating, either on a fixed maintenance cycle (e.g., monthly) or based on some regular cycle after a patch is released?

Choose a single value for each row. If multiple values are appropriate depending on system type, choose the shortest interval Mark only one oval per row.

	2 Days	1 Week	1 Month	3 Months	> 3 Months
Critical					
Important					
Moderate					
Low					

17. If your project or facility uses cloud-based services (e.g., source code management), how are accounts managed in that environment?

Check all that apply for any project of facility cloud services

- Integrated with project or facility identity management

- Periodically synchronized with project or facility accounts
- Separate accounts that are independently maintained
- Other:

18. How many cybersecurity incidents (i.e., any event that puts the confidentiality, integrity, or availability of data or information systems at risk) has your project or facility experienced in the past year?

Mark only one oval.

- 1-3
- 4-6
- 7-10
- > 10
- None
- Don't know
- Prefer not to answer

19. What were the impacts of cybersecurity incidents to your project or facility?

Check all that apply

- Loss of reputation
- Decreased confidence in data integrity
- Temporary or permanent inability to collect or analyze data
- Interruption of remote access
- Sanctions or legal actions due to breach of sensitive information
- Significant cost of incident recovery procedures
- Cost of additional remediation procedures / controls
- Does not apply
- Other:

20. For the cybersecurity incidents your project or facility experienced in the past year, which have had the greatest impact?

Check no more than 2

- Network denial of service
- Compromise / failure of servers
- Compromise or infection of workstations
- Compromised / lost / stolen portable devices (mobile phones, laptops)
- Altered or theft of data (including password files or information considered sensitive - pre- publication, HIPAA, PII, non-disclosure information)
- No detected incidents
- Other:

Cybersecurity Concerns

21. What would most improve your project or facility's cybersecurity stature?

Check at most 2

- Advanced security technology (hardware and/or software)

- Cybersecurity steering committee
- Employee/researcher reward / disciplinary systems
- Increased cybersecurity staff
- Larger cybersecurity budget
- Senior Management commitment
- Other:

22. What cybersecurity threats are of most concern to your project or facility?

Check at most 2

- Unauthorized or accidental modification of data
- Exposure of confidential or sensitive information
- Loss of availability or sabotage of systems
- Incorrect network/hardware/software configurations
- Email viruses, ransomware or other malware
- Unauthorized, malicious network/system access
- Other:

23. Comments - Use this space to record any additional or clarifying comments.

Feedback

24. Thank you for your participation in the CTSC Community Survey. If you have any feedback, please feel free to add comments below.

Appendix B: Tables of Survey Results

Project or Facility Budget

Q1. What is your project or facility’s annual budget? [Exclusion is not responsive]

	All	Large Facilities	Big	Small
Range	$70K-$200M	$7M-$200M	$2M-$24M	$70K-$400K
Avg - Mean	$22M	$58M	$13.2M	$175K
Avg - Median	$7M	$28M/37M	$12M	$130K/$160K
Exclusions	1	1	0	0

Q2. What is your project or facility's annual information technology budget? [Exclusions responded zero or not a separate budget item]

	All	Large Facilities	Big	Small
Range	$3K-$25M	$1M-$25M	$550K-$15M	$3K-$100K
Range % Budget	0%-100%	2%-67%	5%-75%	1.7%-100%
Avg - Mean	$3M	$5M	$4.8M	$32K
Avg - Median	$1M	$1.4M/$2.3M	$1M/$4M	$10K-$15K
Median % budget	14.3%	5%	48%	7.5%
Exclusions	7	1	0	6

Q3. What is your project or facility's annual cybersecurity budget? [Exclusions responded zero or not a separate budget item]

	All	Large Facilities	Big	Small[12]
Range	$2K-$3M	$13K-$3M	$0-$1.1M	$2K-$45K
Range % Budget	0.02%-23%	0.02%-1.5%	0.25%-3.9%	---
Avg - Mean	$374K	$442K	$339K	---
Avg - Median	$60K	$75K/$78K	$50K	---
Median % budget	0.5%	0.5%	0.5%	---
Exclusions	11	1	2	10

Project or Facility Attributes

Q4. Is your project or facility an NSF Large Facility?

Yes	9
No	17
Don't know	0

Q5. Do individuals from multiple institutions authenticate to the resources of your project or facility?

	All	Large Facilities	Big	Small
2 or 3	5	2	1	2
More than 3	14	7	5	2
No	6	0	1	5
Don't know	1	0	0	1

[12] Only 2 responses so statistics not meaningful

Q6. Does your project or facility have a person with defined authority for developing and maintaining a cybersecurity program (e.g., ISO, CSO, CISO)?

	All	Large Facilities	Big	Small
Full-time	1	1	0	0
Part-time	11	6	5	0
No	14	2	2	10
Don't know	0	0	0	0

Q7. Is there an identifiable group devoted to cybersecurity within your project or facility?

	All	Large Facilities	Big	Small
In IT	13	7	4	2
Not in IT	2	1	0	1
No	11	1	3	7
Don't know	0	0	0	0

Q8. Does your project or facility develop or maintain software? If so, what policies, processes or tools do you use? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Coding Standards	17	6	5	6
Interpreted Languages	20	7	5	8
Compiled Languages	23	9	7	7
Source Code Repositories	26	9	7	10
Automated Testing	17	7	5	5
Continuous Integration	15	6	4	5
Static/Dynamic Analysis	8	3	3	2
Issue Tracking / Vulnerability Management	20	8	7	5
Testing Policies	13	4	6	3
Code Signing	6	2	3	1
Automated Documentation	10	3	5	2
Not applicable	0	0	0	0

Cybersecurity Program

Q9. How are cybersecurity policies developed and officially adopted within your project or facility? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
IT or Cybersecurity	13	7	5	1
Governance Board	7	4	2	1
PI or Project Leadership	11	1	6	4
No Process	6	0	1	5
Host Institution	11	4	4	3

Q10. What framework or guidance (if any) has your project or facility adopted for how cybersecurity is done? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
CIS	2	2	0	0
NIST RMF	8	5	3	0
CTSC Guide	5	3	2	0
None	12	1	2	9
“IGTF”	1	0	0	1

Q11. Who accepts residual cybersecurity risk (i. e., the remaining risk after reasonable cybersecurity controls are established)? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Cybersecurity person	0	0	0	0
IT Manager	3	0	1	2
System/Process Owner	1	1	0	0
SeniorManager or PI	8	3	3	2
No Process	13	5	3	5
No Response	1	0	0	1

Q12. What external cybersecurity requirements (if any) are imposed on your project or facility? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
PII	7	3	2	2
PHI	2	2	0	0
NDA or contractual	4	3	1	0
Classified	1	1	0	0
FISMA	1	1	0	0
Cooperative Agreement	10	8	2	0
None	5	1	1	3
Don’t Know	3	0	0	3
“WLCG”	1	1	0	0
“MOU”	1	0	1	0
“IGTF”	1	0	0	1
“Host Institution”	1	0	0	1

Q13. What kind(s) of identity management does your project or facility employ to control access to its resources? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Parent Institution	10	2	2	6
Project Provided userid/pswd	16	7	5	4
Project Certificate	8	2	3	3
Federated IDM	7	3	3	1

Q14. What programmatic cybersecurity safeguards has your project or facility implemented? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Maturity Models	2	1	1	0
Strategy, policy or plan	11	7	3	1
Documented standards or baselines	12	7	4	1
Risk assessments	11	7	4	0
Inventory critical assets	9	5	3	1
Monitor security intelligence	7	4	3	0
Cyber incident response plan	12	8	3	1
Improvement roadmap	8	5	3	0
Data classification	8	5	3	0
Periodic awareness training	9	6	2	1
Disaster recovery plans	12	7	4	1
Governance structure	8	6	2	0
External review	8	5	2	1
None	8	0	0	8

Q15. What operational cybersecurity safeguards has your project or facility implemented? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Multi-Factor Authentication	7	2	3	2
Centralized logging	15	8	6	1
Data Loss prev / encryption	9	3	3	3
Vulnerability management	11	7	4	0
Intrusion detection	11	7	3	1
Anti-virus, spam, phishing	12	8	3	1
Real-time alerts	9	5	3	1
Physical access controls	16	8	5	3
Firewalls	18	9	5	4
Vulnerability scans	13	7	4	2
Tabletop exercises	4	3	1	0
Penetration or phishing testing	5	3	2	0
None	4	0	0	4

Q16. How frequently are patches applied based on the severity rating, either on a fixed maintenance cycle (e.g., monthly) or based on some regular cycle after a patch is released?

D/W/M/3M/>3	All	Large Facilities	Big	Small
Critical	12/10/0/0/0	5/3/0/0/0	5/2/0/0/0	2/5/0/0/0
Important	1/15/5/0/0	0/7/1/0/0	0/5/2/0/0	1/3/2/0/0
Moderate	0/4/11/2/3	0/2/6/0/0	0/1/3/1/1	0/1/2/1/2
Low	0/2/7/6/7	0/1/5/2/0	0/0/0/3/4	0/1/2/1/3

Q17. If your project or facility uses cloud-based services (e.g., source code management), how are accounts managed in that environment? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Integrated w/ Project	5	3	2	0
Periodically Sync'ed	1	0	1	0
Separate Accounts	14	4	2	8
N/A or No Response	7	2	3	2

Q18. How many cybersecurity incidents (i.e., any event that puts the confidentiality, integrity, or availability of data or information systems at risk) has your project or facility experienced in the past year?

	All	Large Facilities	Big	Small
1 - 3	12	7	4	1
4 - 6	0	0	0	0
7 - 10	0	0	0	0
> 10	0	0	0	0
None	13	2	3	8
Don’t Know	1	0	0	1
Prefer not to answer	0	0	0	0

Q19. What were the impacts of cybersecurity incidents to your project or facility? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Loss of Reputation	1	0	1	0
Decreased confidence in data	1	0	1	0
Inability to collect / analyze data	1	0	1	0
Interrupt remote access	4	3	1	0
Sanctions or legal action	0	0	0	0
Significant cost of recovery	1	1	0	0
Cost of remediation	2	2	0	0
Does Not Apply	17	3	4	10
No Response	2	1	1	0
“Individual Workstation”	1	1	0	0
“False Alarm”	1	1	0	0
“Suspend Accounts”	1	0	1	0

Q20. For the cybersecurity incidents your project or facility experienced in the past year, which have had the greatest impact? [Respondents allowed to select no more than two.]

	All	Large Facilities	Big	Small
Network denial of service	1	0	1	0
Compromise server	2	1	1	0
Compromise workstation	5	4	1	0
Compromised portable device	1	1	0	0
Altered or theft of data	0	0	0	0
No detected incidents	14	2	4	8
No response	2	1	0	1
“External power loss	1	1	0	0
“Account compromise”	1	0	1	0
“Unauthorized access”	1	0	0	1

Cybersecurity Concerns

Q21. What would most improve your project or facility's cybersecurity stature? [Respondents allowed to select no more than two.]

	All	Large Facilities	Big	Small
Advanced technology	5	1	2	2
Cybersecurity steering committee	4	3	1	0
Reward / disciplinary Systems	5	2	1	1
Increased staff	9	4	2	3
Larger budget	9	3	3	3
Senior management commitment	4	2	2	0
No Response	3	1	0	2
"Malware awareness"	1	1	0	0
"Depend on host university"	1	0	0	1

Q22. What cybersecurity threats are of most concern to your project or facility? [Respondents allowed to select no more than two.]

	All	Large Facilities	Big	Small
Modification of data	11	3	4	4
Exposure of sensitive information	6	2	2	2
Loss of availability or sabotage	10	6	2	2
Incorrect configurations	4	0	2	2
Viruses, ransomware, malware	7	4	0	3
Unauthorized access	10	2	4	4
No Response	1	0	0	1
“No concern for such open source, small scale project”	1	0	0	1

Comments

Q23. Use this space to record any additional or clarifying comments.

A Large Facility	"Our predominant concerns would be loss of observation time (instrument taken down) due to remediation efforts or damage to the instrument itself. Data integrity is an issue, but we deal with that in a number of ways already. Confidentiality is not a primary concern given the unique nature of the data set. So while our data is not made public immediately, a premature disclosure due to a security incident (or any other type of incident) does not incur direct regulatory or penalty costs."
A Small project	"We depend on the hosting university for improvements; little concern for threats on such a small project"