



Columbus State University
CSU ePress

Theses and Dissertations

Student Publications

12-2020

Proactive Management in Academic Libraries: Promoting Improved Communication and Inclusion of Academic Librarians and Archivists in Cybersecurity Policy Creation

Paul J. Luft

Follow this and additional works at: https://csuepress.columbusstate.edu/theses_dissertations



Part of the [Computer Sciences Commons](#)

COLUMBUS STATE UNIVERSITY

PROACTIVE MANAGEMENT IN ACADEMIC LIBRARIES
Promoting Improved Communication and Inclusion of Academic
Librarians and Archivists in Cybersecurity Policy Creation

A THESIS SUBMITTED TO
THE TURNER COLLEGE OF BUSINESS
IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF CYBERSECURITY MANAGEMENT
TSYS SCHOOL OF COMPUTER SCIENCE

BY
PAUL J. LUFT

COLUMBUS, GEORGIA

2021

Copyright © 2020 Paul J. Luft

All Rights Reserved.

PROACTIVE MANAGEMENT IN ACADEMIC LIBRARIES:
Promoting Improved Communication and Inclusion of Academic
Librarians and Archivists in Cybersecurity Policy Creation

By

Paul J. Luft

Committee Chair:

Dr. Lydia Ray

Committee Members

Dr. Shamim Khan

Dr. Yesem Kurt Peker



Jacqueline Radebaugh

Columbus State University

December 2020

ABSTRACT:

Although increasing cybersecurity threats continue in libraries, not many studies are available which examine surrounding cybersecurity policies. Even less has been done on specific types of libraries such as academic and archives. When it comes to academic libraries, cybersecurity policies take a top-down approach to managing and creating policies. The problem is that both academic libraries and archives are unique areas within a university setting. Some of the general policies do not always handle specific issues dealt with in an academic library or archives. This paper investigates if an actual gap or void in policy exists which could create issues in academic libraries and archives, as well as if the university cybersecurity policy is being communicated, reviewed, reported, and created with inclusion of librarians and archivists. An 18-question survey was administered to librarians, archivists, and university information technology cybersecurity professionals within the 24 academic institutions of University Systems of Georgia (USG). Twenty-seven respondents completed the survey. The survey was, then, analyzed according to subcategories. A general theme emerged: communication of cybersecurity policy and the inclusion of librarians and archivists in policy creation and reporting could improve cybersecurity defense. The lack of participation and report feedback also lead to a very low perception or barometer score (5.1 average on a 10-point scale) as to how well the cybersecurity plan was being communicated. The solution to the communication gap could be in form of a plan. A conceptual model entitled Communication Enlightenment Engagement Plan (CEEP) would increase involvement by community engagement (inclusion, policy review, and policy creation.) Adding a feedback loop to CEEP will aid in the engagement process as well as keeping top tiers of management aware of policy changes and issues.

INDEX WORDS: Cybersecurity Policy, Libraries Cybersecurity, Libraries Cybersecurity Threat, Cybersecurity Management, Cybersecurity Plan

ACKNOWLEDGMENTS

I would like to thank my wife, Muriel, for her understanding and encouragement she has provided to me throughout this entire master's program. She is an outstanding proofreader. I am deeply thankful for her aid in proofing this paper.

Next, I would like to thank Dr. Lydia Ray for being an exceptional instructor, advisor, and mentor. I have enjoyed the presentation and lectures from Dr. Ray's lessons. She can break down complicated issues and provide insight along with encouraging student participation. She allows students to share real-world experiences with the class, which serves as a way to get to know fellow students and, possibly, lead to future friendships. I have learned some pedagogy lessons from her as well, because someday I hope to teach others. I have also found her to be a helpful advisor when I needed to ask her questions about career paths.

I would, additionally, like to thank all the librarians, archivists, and cybersecurity personnel from within the University Systems of Georgia who took the time to fill out my survey.

Finally, I would like to thank my classmates for encouragement and our healthy debates on cybersecurity issues. Without those debates, I might not have developed some of my cybersecurity management knowledge.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	iv
LIST OF TABLES	viii
LIST OF FIGURES	ix
1. INTRODUCTION	1
1.1 PROBLEM STATEMENT	2
1.2 BACKGROUND INFORMATION	2
1.3 LITERATURE REVIEW	3
1.31 WHAT ARE THE ISSUES SURROUNDING UNIVERSITY LIBRARIES AND CYBERSECURITY?	3
1.32 LIBRARIANS AND POLICY	3
1.33 BALANCING PRIVACY AND DATA COLLECTION	4
2.0 Detail Review of University Systems of Georgia Information Technology Services Policy (Tier 1) and Issues with Communication Framework at the University and Library Level (Tier 3)	5
2.1 POINT 1: (FAIR REPRESENTATION)	5
2.2 POINT 2: (CLEARLY DEFINED OUTCOMES)	6
2.3 POINT 3: (WELL-DEFINED COMMUNICATION OF FRAMEWORK)	6
2.4 POINT 4: (REVIEW OF STANDARDS)	7
2.5 POINT 5: (UNIVERSITY LIBRARY-LEVEL CYBERSECURITY POLICY – DOES IT EXIST?)	7
3.0 Issues with Each Point Explained (Each Point will be addressed)	7
3.1 POINT 1: FAIR REPRESENTATION	7
3.2 POINT 2: CLEARLY DEFINED OUTCOMES	8
3.3 POINT 3: WELL-DEFINED COMMUNICATION OF FRAMEWORK	8

3.4 POINT 4: REVIEW OF STANDARDS	8
3.5 POINT 5: UNIVERSITY LIBRARY-LEVEL CYBERSECURITY POLICY – SHOULD IT EXIST?	8
3.6 AN ADDITIONAL POINT: WORKING LIBRARY ENVIRONMENT (TIER 3)	9
4.0 ARRIVAL OF THE PROBLEM STATEMENT	10
4.1 THUS, THE PROBLEM STATEMENT	10
5.0 Study of University of Georgia (USG) System Librarians, Archivist, and Cybersecurity Information Specialist	11
6.0 Results and Discussion of the Survey	12
6.1 ANALYSIS OF SECTION 1: BACKGROUND INFORMATION (2 QUESTIONS)	12
6.2 ANALYSIS OF SECTION 2: PRIORITIZING AND AWARENESS OF CYBERSECURITY THREATS (2 QUESTIONS)	13
6.3 ANALYSIS OF SECTION 3: DIRECT COMMUNICATION OF POLICY (3 QUESTIONS)	17
6.4 ANALYSIS OF SECTION 4: CYBERSECURITY POLICY CREATION OR PARTICIPATION (4 QUESTIONS)	20
6.5 ANALYSIS OF SECTION 5: REPORTING PROCEDURES (2 QUESTIONS)	21
6.6 ANALYSIS OF SECTION 6: THINGS THAT GET LEFT OUT (1 QUESTIONS)	23
6.7 ANALYSIS OF SECTION 7: OVERALL REFLECTIVE BAROMETER (1 QUESTIONS)	24
6.8 SURVEY IMPROVEMENT CONSIDERATIONS	25
7.0 SURVEY CONCLUSION	25
7.1 Cybersecurity Communication Gap	26
7.2 Cybersecurity Policy Inclusion and Creation	27
7.3 Cybersecurity Reporting and Feedback	27
7.4 Policy Improvement	29
7.5 Summary Recap	30

8.0 PROPOSED POLICY SOLUTION OF COMMUNICATION ENLIGHTENMENT ENGAGEMENT

PLAN (CEEP)	31
9.0 CONCLUSION	34
REFERENCES	36
APPENDICES	
APPENDIX A: COLUMBUS STATE UNIVERSITY POLICY REVIEW & NIST	37
APPENDIX B: LIBRARY CYBERSECURITY COMMUNICATION SURVEY	41
APPENDIX C: QUESTION 4 – RAW DATA	48

LIST OF TABLES

<i>Table 1: Perceived Cybersecurity Threat Data</i>	13
<i>Table 2: Cybersecurity Survey Comments</i>	23
<i>Table 3: Barometer Rating Responses</i>	24
<i>Table 4: Highest Variance Rates Amongst Cybersecurity Threats</i>	25
<i>Table 5: Reporting/Feedback/Status Reports</i>	28





LIST OF FIGURES

<i>Figure 1: University Policy Hierarchy</i>	3
<i>Figure 2: Survey Correspondents Makeup</i>	12
<i>Figure 3: Cybersecurity Prioritization</i>	14
<i>Figure 4: Cybersecurity Threat Awareness</i>	17
<i>Figure 5: Cybersecurity Department Communication</i>	17
<i>Figure 6: Cybersecurity University Policy Familiarization</i>	18
<i>Figure 7: Cybersecurity Policy Review</i>	19
<i>Figure 8: Cybersecurity Policy Communication After Changes</i>	19
<i>Figure 9: Cybersecurity Inclusion in Policy Creation</i>	20
<i>Figure 10: Cybersecurity Policy Inclusion</i>	20
<i>Figure 11: Cybersecurity Policy Review Frequency</i>	21
<i>Figure 12: Cybersecurity Occurrence</i>	21
<i>Figure 13: Report Feedback Loop</i>	22
<i>Figure 14: Cybersecurity Awareness of Possible Threats</i>	22
<i>Figure 15: Network Health Status</i>	23
<i>Figure 16: Cybersecurity Barometer</i>	24
<i>Figure 17: Communication Barometer</i>	31
<i>Figure 18: CEEP Conceptual Model</i>	32
<i>Figure 19: Report Feedback Loop</i>	33

PROACTIVE MANAGEMENT IN ACADEMIC LIBRARIES:
Promoting Improved Communication and Inclusion of Academic
Librarians and Archivists in Cybersecurity Policy Creation
A thesis submitted to Turner School of Business
in partial fulfillment of the requirements for the degree of
MASTER OF CYBERSECURITY MANAGEMENT

TSYS OF COMPUTER SCIENCE

By
Paul J. Luft
2021

 _____	<u>1/11/2021</u>
Dr. Lydia Ray, Chair	Date
 _____	<u>3/11/2021</u>
Dr. Shamim Kahn, Member	Date
 _____	<u>1/14/2021</u>
Dr. Yesem Kurt Peker, Member	Date
 _____	<u>03/12/2021</u>
Jacqueline Radebaugh, Member	Date

1. Introduction

Libraries are one of the most overlooked areas of cybersecurity. This author often wonders why this is so. Is it because libraries do not deal with banking or health information? Instead, libraries do deal with private information. Additionally, some people utilize libraries' computers to do many transactional-type actions such as tax returns, motor vehicle registration, student loans, e-mails, etc. Often overlooked is the wealth of copyrighted academic knowledge held in the databases that could be collected without permission. Digital collections that hold historical information could also be corrupted.

Education information systems and university libraries are seeing an increased number of data breaches, ransomware, and hacking attempts (Henig, p. 6, 2018). An estimated 171 million Americans are registered to a library (Rocca & Burkhard, p. 1, 2019). Every day, thousands of people walk into a library with the expectation of utilizing the resources available to them. Some of these users bring with them devices to link to the network, while others just want to use the resources that the library offers them (computers, network, electronic databases, digital collections, etc.). These patrons do not want to wrestle with security issues to the extent that their workflow becomes impeded. The American Library Association (ALA) describes cybersecurity and libraries as user-friendly, because all library resources should be readily accessible and privacy secured (ALA, 2016). For this reason, the library has had a relaxed posture with cybersecurity and, thus, has been the target of cybersecurity attacks and hacks.

The article "Should libraries consider hacking back if attacked?" demonstrates the increasing frustrations from cyber-attacks. Some noteworthy attacks are: Aaron Schwartz, who downloaded 4 million academic articles from MIT; and another case, where a new electronic textbook was altered to refer to slaves as unpaid interns (Smith, p.15, 2017). Smith is correct in

pointing out that Archival digital collections within libraries' collections are vulnerable, because they are housed on different systems (Smith, p.15, 2017). For example, the Columbus State University system's digital collection is not on the same platform as the library's e-books and other collections.

1.1 Problem Statement

Considering the previously mentioned user-friendly and privacy concerns along with increasing attacks coupled with multiple information systems running on the university network, this explains why a general cybersecurity policy is difficult and, sometimes, in conflict with the library's cybersecurity policy. Additionally, an attitude exists that University Information Technology Systems do not include the system librarians in policy and issues surrounding cybersecurity. This project intends to explore and determine if there is evidence of a disconnect in communication and policy creation between Librarians, Archivists, and University Information Technology Systems in an academic setting such as the University Systems of Georgia. This disconnect in communication of policies and current threats awareness can cause the library to be vulnerable to cyberattacks.

1.2 Background Information

To understand the governance and communication issue of University Libraries, of vital importance is to understand the tiers of how a technology policy is created and could be governed. At Tier 1, the University System of Georgia Information Technical Service (USGITS) creates policy for all information technical services (discussed more in "Details" section). At Tier 2, each and every individual information technical service department is depicted. Lastly, the system library, or library department, along with archives will be labeled Tier 3. This demonstrates a top-down approach as to how cybersecurity policy is governed (See Figure 1).

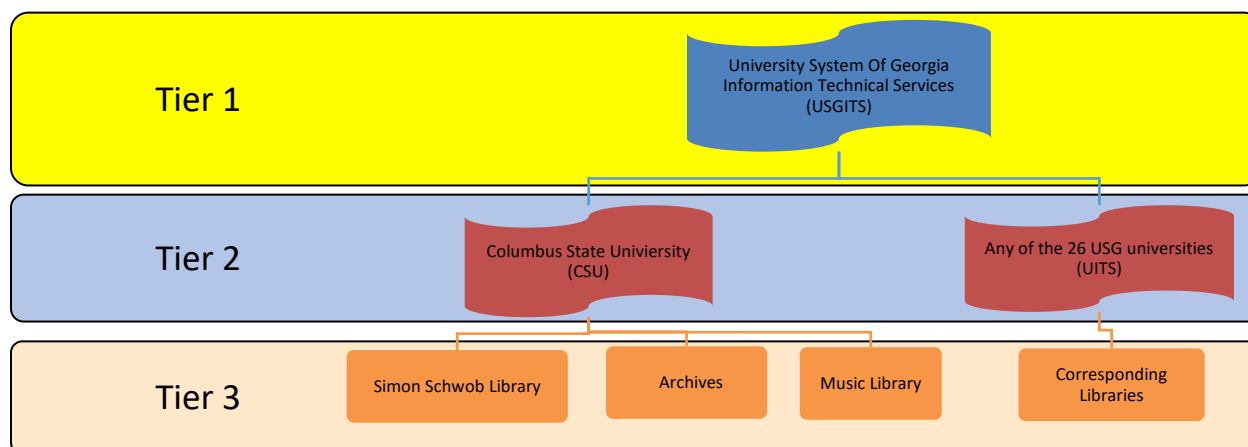


Figure 1: University Policy Hierarchy

1.3 Literature Review

1.31 What are the issues surrounding university libraries and cybersecurity?

Physical security is an important role in cybersecurity, just as it is in large corporations. Things such as natural disasters (fire, flood, tornado, earthquake, building collapse), vandalism, air conditioner failure, etc., all affect hardware assets (Aije, p. 5 & 12, 2019). Along with these hardware vulnerabilities comes software vulnerabilities. This can take many forms such as trojans, worms, viruses, password sniffing hacking, spyware, adware, etc. (Aije, p. 6-7, 2019). Additionally, data security threats can be present which range from destruction of resources, corruption of information, theft in removal of other resources, interruption of services to changing data, data loss, delay of dissemination, loss of privacy, copyright violations, and natural disaster (Aije, p. 10, 2019). Furthermore, human error may be involved, including incorrect set-up of security features, incorrect switching off equipment, deletion of files, inadequate back-ups, and improper following of procedures (Aije, 2019).

1.32 Librarians and Policy

Besides Landgraf, the other two articles, Aije and Rudasill, have highlighted policy issues surrounding libraries. Aije points out that university libraries' issues with cybersecurity require

“serious managerial and strategic attention.” (Aije, p. 17, 2019). Additionally, librarians need to be included in policy and regulation decisions (Rudasill & Moyer, p. 254, 2004).

1.33 Balancing Privacy and Data Collection

As stated in the introduction, patrons do not want their privacy violated. The University of Arizona collected data swipes of IDs to predict retention, progression, and graduation (Landgraf, p. 1, 2018). The American Library Association has been on the side of Academic Freedom and Privacy since it was founded, so much so, that it is coded in the Library Bill of rights, found at <http://www.ala.org/advocacy/intfreedom/academicfreedom>. The Right to Privacy can be found in Article VII of the ALA Bill of Rights which states, “All people, regardless of origin ... The right to privacy is the right to open inquiry without having one’s interest examined or scrutinized by others ... Confidentiality relates to records, computer sign-up sheets, websites visited ...” The problem occurs when data is required, by administration, for the library to prove that it is being utilized and/or what is being utilized for funding, which this paper is not going to examine. This point leads us to that which Landgraf elucidates: a regulatory framework relating to policy needs to be updated to keep up with modern times (Landgraf, p. 2, 2018).

Additionally, a video produced by the Higher Education Information Security Council (HEISC), entitled *Campus cybersecurity teams face a broad range of challenges today*, explains the value of education data and the increasing number of attacks laying siege on campuses. According to Bates et. al., the nine key challenges that education faces are as follows:

- 1) Sheer volume of digital assets,
- 2) Threat landscape more complex,
- 3) Intrusive data collection of social media,
- 4) Lax of internet of things devices (security - convenience versus security),
- 5) Continued growth compliance obligations,
- 6) Difficulty to retain and train staff,
- 7) Password reuse,
- 8) Risk management in the cloud, and
- 9) Balancing the open environment of education (Bates et. al., 2019).

As one can see, many themes begin to merge. Users want the freedom to access the network and be private. However, in doing so, security gaps can be created that pertain to the data being stored on the network.

2.0 Detail Review of University Systems of Georgia Information Technology Services Policy (Tier 1) and Issues with Communication Framework at the University and Library Level (Tier 3)

The literature review provides significant evidence that library security policy is lacking, and the threat landscape is dangerous. To understand the lack of a cybersecurity policy as a problem, it might be useful to, first, understand organization structure and policies at each level of a large university system. In this case, we will use University Systems of Georgia Information Technical Services (USGITS - https://www.usg.edu/information_technology_services/), Columbus State University Information Technical Services (CSUITS), and the Columbus State University Simon Schwob Libraries (CSUSSL).

Starting at the head of the institution of USGITS, one can examine the policy handbook, found at https://www.usg.edu/assets/information_technology_services/documents/2020_IT_Handbook.pdf, located on the webpage https://www.usg.edu/cybersecurity/policies_and_reports.

What is interesting is that in both the USGITS webpage and in the introduction of the handbook it mentions this statement: “As noted in Section 5.2.2 of the [Information Technology Handbook](#), USG institutions, the USO, the GPLS, and the Georgia Archives are responsible for the designation of officials within their organization to fulfill key security functions and report on its status of compliance with security policy, standards and procedures.” – (Board of Regents of University of Georgia (BRUG), 2020)

2.1 Point 1: (Fair Representation)

It is unclear if a university library delegate is represented in the creation of these policies and procedures. The above statement from Section 5.2.2 reads that a university representative,

archival representative, and a general public librarian are part of the policy creation. NIST Framework 1.0, Framework Introduction, addresses stakeholders as critical members of the community (NIST, p. 1, 2018). One might argue this is somewhat covered in 1.2.1 (identify) of the Information Technology Handbook (ITH), which states that stakeholders of the organization will participate and have shared responsibilities to assure resource needs. (Discussion continues within *Issues With Each Point Explained (IWEPE)* Section Point 1 of this paper.)

2.2 Point 2: (Clearly Defined Outcomes)

Section 5.5 states, “The USG CISO shall also maintain risk management implementation standards that the USG organizations must consider in the development of their individualized risk management plans.” Much of what is first written pertains to risk management. The goals are not clearly stated; however, what is stated in this section are the activities that the organization will follow. (Discussion continues within *(IWEPE)* Section Point 2 of this paper.)

2.3 Point 3: (Well-Defined Communication of Framework)

It is hard to determine if there is a *formal* communication plan. The ITH mentions, throughout, who reports to whom. Additionally, the ITH mentions what reports and forms are to be filled out. (Discussion continues within *(IWEPE)* Section Point 3 of this paper.)

The policy on the institutional level has been examined. Now, the policy at the singular university level must, also, be examined. Paul Luft examined the NIST standards at Columbus State University and wrote a report which is listed in Appendix A. The main point is this:

Review of 27 Information Security Policies at Columbus State University,
Columbus, GA, were paired with NIST standards found at
<https://nvd.nist.gov/>. The 5 controls that are either deficient or missing (will

be further explained) are [AC-10](#), [AC-11](#), [AC-12](#), [AC-18](#), and [AC-19](#). Twenty controls were found in accordance with NIST STANDARDS.

2.4 Point 4: (Review of Standards)

Who is reviewing the standards between the tiers? Are they just reviewing the standards at the university to NIST, or to the institutional policies, or to both? (Discussion continues within *IWEPE* Section Point 4 of the paper.)

2.5 Point 5: (University Library-Level Cybersecurity Policy –Should It Exist?)

Very few university libraries have their own cybersecurity policy. Indiana University (I.U.) has a library cybersecurity policy located at <https://policies.iu.edu/policies/lib-01-libraries-privacy/index.html>. This policy, and most other university libraries which have cybersecurity policies, contains a statement that reads something like, “This library adheres or follows the university IT policy.” The I.U. library cybersecurity policy has a section dedicated to privacy rights, third-party software, and data destruction. (Discussion continues *IWEPE* Section Point 5 of the paper.)

3.0 Issues with Each Point Explained (Each Point will be addressed)

3.1 Issue with Point 1: Fair Representation

When an organization gets large, with many branches located in different geographical places, this organization must have fair representation during policy and procedure creation. This author believes that USGITS has not accomplished this with their *1.2.1 Shared Governance Framework* (*ITH, p.12, 2020*).

3.2 Issue with point 2: Clearly Defined Outcomes

If other Information Technology Service departments throughout the USG system are to use this document to develop or adapt policy, an easy way needs to exist to find the clear objectives concerning cybersecurity. This document was not easy to follow.

3.3 Issue with point 3: Well-Defined Communication of Framework

A formal structure of who reports to whom and what reports are to be filled out must be defined, along with an assessment cycle defined as to when reports are due. Unfortunately, how other facilities fit into this structure is hard to see. Therefore, a diagram is needed to understand and illustrate the communication process, such as the one seen in the NIST Framework for Improving Critical Infrastructure.

3.4 Issue with point 4: Review of Standards (Tiers 1, 2, 3 & NIST)

Cybersecurity policy review is occurring, and USGITS updates their handbook. As stated per policy, communication of those changes is being passed on to the CIOs. The CIOs, then, ensure that these processes are being written into current policy and, subsequently, communicated to the university departments (Tier 3) that utilize the network (like the library). However, nowhere are notification of standards and changes communicated to departments at the university level. It is safe to assume that this notification process falls on the responsibility of the University ITS to communicate these changes. A formal communication plan would assure that communication to departments has been received. This is an important point, because it leads into Point 5.

3.5 Issue with point 5: University Library-Level (Tier 2) Cybersecurity Policy – Should It Exist?

While not many university libraries' have cybersecurity policies, some libraries have cybersecurity policies in addition to UITS. UITS and USGIT policy do not appear to handle the

working environment of the library. The fact that the library at IU had to draft a policy on privacy, third-party software, and data destruction separate from the UITS should demonstrate the need for librarians to be part of the UITS cybersecurity policy. The working environment is more complex than just device linkup on the network.

3.6 An Additional Point: Working Library Environment (Tier 3)

In examining the cybersecurity policies at the university level (Tier 3), no policies or procedures were found regarding what to do when devices are found without an owner in the library, such as thumb drives. Thumb drives are left behind by students on a regular basis. Nowhere within the policy are statements regarding how to handle these types of items. Typically, a library worker will plug a thumb drive into a library computer to try to find its owner. This can be dangerous, because somebody may have perpetrated a malicious act by planting a virus onto the network in this manner.

Next is the examination and inspection of equipment. Nowhere was listed guidance from UITS about laptops, Chromebooks, or phone cables that were checked out by a student and, later, returned. Malicious software or hijacking software could be placed on this equipment. Yes, UITS has installed safeguards, so that students cannot install software. Nevertheless, what if a student was clever enough to put a hijacking piece of equipment onto the laptop or charger cord. This has been done with cell phone charger cords (which some libraries allow to be checked out). This illustrates the point that, without a librarian on the cybersecurity policy creation side of things, there will be no policy about this type of attack. Libraries formulate their own policies and procedures regarding how to handle these things without guidance from cybersecurity experts.

4.0 Arrival of the Problem Statement

Plenty of evidence demonstrates that university libraries lack cybersecurity policies to deal with the changing threats, as stated in the literature review. Additionally, users of the library, along with the ALA, almost demand “user-friendly” access to the network. The daily issues and pressures on the library can only be understood by those who work in the library. Policy development takes place two tiers up in the University of Georgia Systems, without inclusion of a university librarian. Public librarians have been consulted, but their needs and functions are very different than those of university librarians. To add even more confusion, the archives are represented which also have different concerns than those of a university library. A viable solution would have a university systems librarian sit on the panel of policy makers.

Additionally, a systems librarian should be part of the cybersecurity policy at the university level, at the very least (Tier 2). If this were to occur, then at least the CIO at the university level would be aware of the cybersecurity and workflow struggles of the library. Furthermore, this would aid in policy implementation, training, and awareness of cybersecurity within library staff. While this paper did not research library staff training and awareness, articles have been written about this topic which also led to the conclusion of a lack of training and awareness of library staff.

4.1 Thus, The Problem Statement

This project intends to explore if there is evidence of a disconnect in communication and policy creation between Librarians, Archivists, and University Information Technology Systems in an academic setting such as the University Systems of Georgia. This disconnect in communication of policies and current threats awareness can cause the library to be vulnerable to cyberattacks.

5.0 Study of University of Georgia (USG) System Librarians, Archivist, and Cybersecurity Information Specialist

A survey was conducted of System Librarians, Archivists, and Cybersecurity Information Specialists within the 24 academic institutions with the University System of Georgia (USG). The survey had 7 sections, with 16 questions devoted to understanding the issues of communication and policy creation as they pertain to cybersecurity policy within academic libraries and archives. The survey sections are as follows:

- Standard informed Consent (1 Question)
- Section 1: Background Information (2 Questions)
- Section 2: Prioritizing and Awareness of Cybersecurity Threats (2 Questions)
- Section 3: Direct Communication of Policy (4 Questions)
- Section 4: Cybersecurity Policy Creation or Participation (3 Questions)
- Section 5: Reporting Procedures (4 Questions)
- Section 6: Things that get left out (1 Question)
- Section 7: Overall Reflective Barometer (1 Question)

For full details of the Qualtrics Survey refer to *Appendix B*.

All participants remained anonymous, and Qualtrics' settings for recording the http address were turned off. All questions were optional, and participants were permitted to exit the survey at any time (Please see *Appendix B* - Informed Consent Section). Additionally, very job-specific participants were chosen for this survey. This means that these individuals were the most likely to participate in the culture of cybersecurity policy creation. For example, a systems librarian would be more likely to handle databases and network issues than a subject-specialist or service-type librarian. Likewise, a cybersecurity information technology specialist is more likely to manage, create, and distribute cybersecurity policy than a general help-desk information assistant. This is important, because the objective is to gauge library cybersecurity policy communication, creation, and participation.

6.0 Results and Discussion of the Survey

Qualtrics-provided report and crosstab functions were utilized to provide the results.

Abbreviations refer to the following:

SL = System Librarian

CIT = Cybersecurity Information Technologist

A = Archivist

Qx = Question and (x) is a placeholder for a number that would be used, for example Q2 would be Question 2

6.1 Analysis of Section 1: Background Information (2 Questions)

Q1 Please identify which of the following group you belong to:

Q1 reveals a study group composed of 19 System Librarians, 7 Archivists, and 7 Cybersecurity Information Specialists.

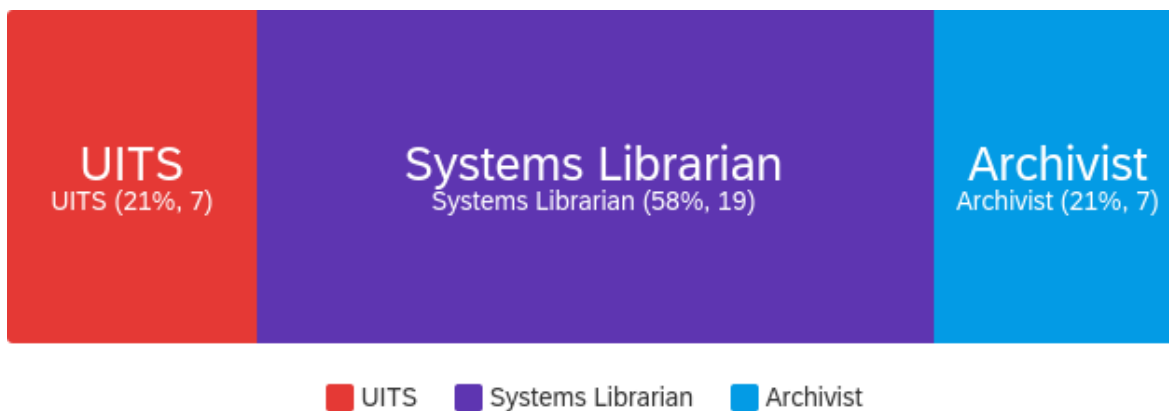


Figure 2: Survey Correspondents Makeup

Q2 pertains to which academic institution the participant belongs. Significant difference is noted between the number of participants and the names of institutions. This could be attributed to the nature of the subject. Participants may be somewhat skeptical about Qualtrics tracing the responses back to the participant.

Q3 was screened and omitted before the survey was conducted. This question seemed like either a repeat or ambiguous, as it related to question 4. It was, therefore, omitted.

6.2 Analysis of Section 2: Prioritizing and Awareness of Cybersecurity Threats

(2 Questions)

Q4 - Rank the following 22 cybersecurity concerns as according to priority, with 0 being the lowest concern and 10 being the highest concern:

High Priority: A cybersecurity threat that you perceive will likely happen, causing severe issues with workflow and privacy AND no matter what little budget you have, you would put money toward combating the threat.

Medium Priority: A cybersecurity threat that you perceive may happen with consequence to workflow and privacy AND are willing to put some money on a limited budget toward combating the threat.

Low Priority: A cybersecurity threat that is unlikely to happen but still might have consequences to workflow and privacy AND you would only put money toward combating the threat if you had extra money to do so. The total group (SL, CIT, A) prioritized the threats as follows:

This table data can be found in a larger size in **Appendix C**.

Table 1: Perceived Cybersecurity Threat Data

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Ransomware of library systems	1	10	5.58	2.91	8.47	26
2	Unauthorized access of library network	0	10	5.19	2.72	7.39	26
3	Unauthorized access of network from within the library. I.e. Wi-Fi range network	0	10	4.81	2.77	7.69	26
4	Password Protection of library systems	0	10	5.96	2.46	6.04	27
5	Malware on library patron computers	1	10	6.31	2.57	6.6	26
6	Malware from lost & found personal devices such as USB	1	10	5.54	2.79	7.79	26
7	Data Breach from library computers and servers	1	10	5.2	2.98	8.88	25
8	Copyright Infringement of journal databases/thesis/research	1	10	5.54	2.41	5.79	26
9	Copyright infringement of electronic archival material	1	10	5.23	2.68	7.18	26
10	Journal Database theft	0	10	4.31	2.64	6.98	26
11	Digital Collection theft	0	10	4.46	3.21	10.33	26
12	Personal Identification theft associated with university network	1	10	6.76	2.39	5.7	25
13	Personal Identification theft associated with library Wi-Fi	1	10	5.76	2.83	8.02	25
14	Personal Identification theft associated with Library RFID (pretend you have one, if you donate)	1	10	4.48	2.61	6.81	25
15	Personal Identification theft associated Library Accounts	1	10	5.27	2.75	7.58	26
16	Personal Identification theft associated with Archive Accounts	0	10	4.4	3.39	11.52	25
17	Personal Identification theft associated with archive billing and/or outside university request	0	10	4.38	3.3	10.9	24
18	Email phishing attacks (Students and Staff)	1	10	7.81	2.39	5.69	26
19	Man-in-the-Middle Attack (People hijacking or listening in on the network)	1	10	5.24	2.53	6.42	25
20	Network Listening Devices (Library patrons)	0	10	4.88	3.08	9.47	25
21	Equipment Tamper (computer, USB cords, fax machines, wall outlets, charging stations)	0	10	4.73	2.98	8.89	26
22	Archival digital collection protection from corruption or malicious alteration	0	10	5	3.21	10.32	25

Prioritizing Threats All Groups

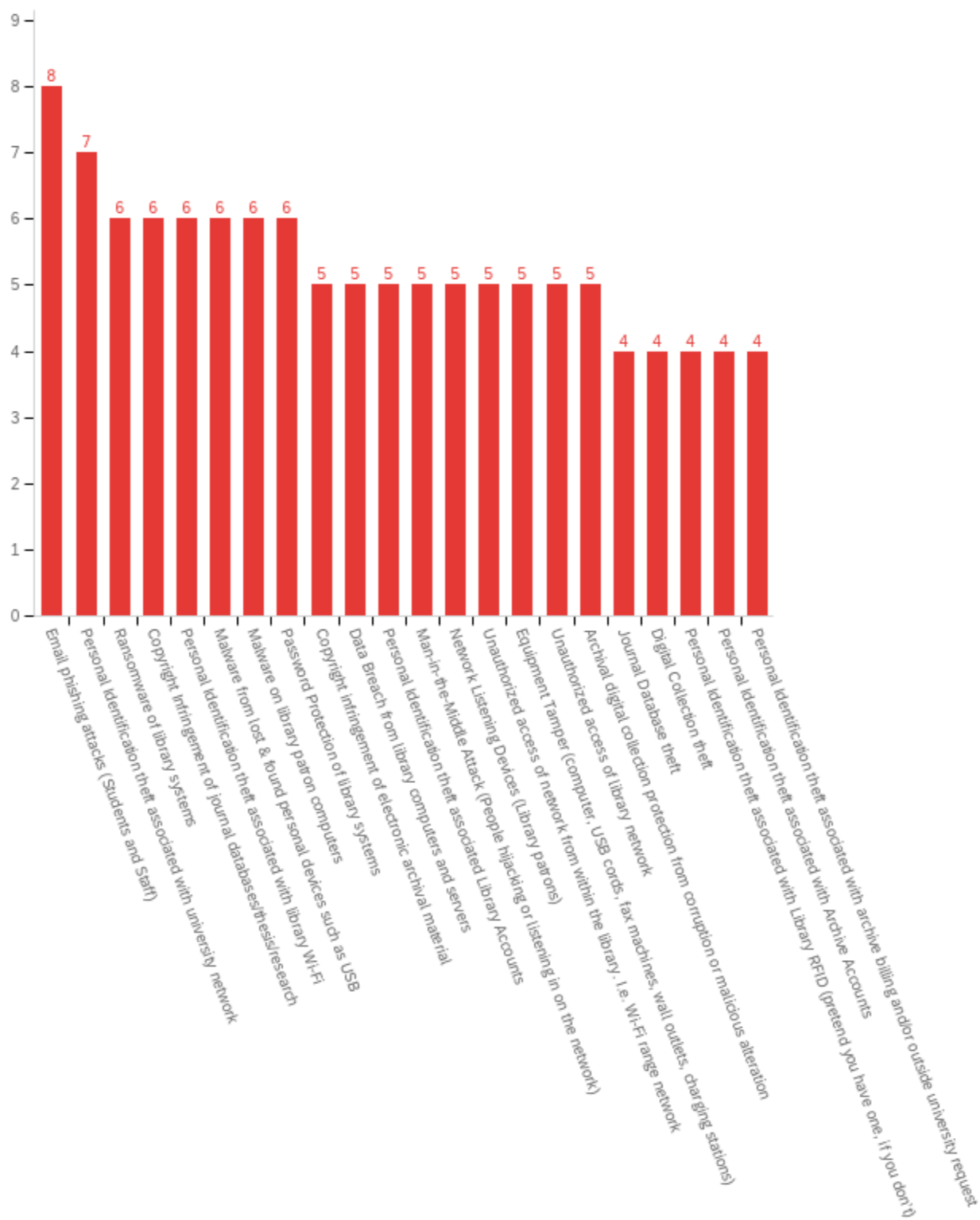


Figure 3: Cybersecurity Prioritization

All three groups identified Email Phishing Attacks as the top concern. This scored a mean score of 8. The next highest concern identified was Personal Identification on Networks which produced a mean score of 7. The third highest concern, with a mean score of 6, was a tie between the following six threats: Ransomware of Library Systems, Copyright Infringement of Journal Databases/Thesis/Research, Personal Identification Theft Associated with Library Wi-Fi, Malware from Lost & Found Personal Devices such as USB, Malware on Library Patron Computers, and Password Protection of Library Systems.

Top Concern - Email Phishing Attacks

Second Top Concern - Personal Identification on Networks

Third Set of Concerns - This set consists of: Ransomware of Library Systems, Copyright Infringement of Journal Databases/Thesis/Research, Personal Identification Theft Associated with Library Wi-Fi, Malware from Lost & Found Personal Devices such as USB, Malware on Library Patron Computers, and Password Protection of Library Systems.

Middle Set of Concerns - The next section has been labeled the middle set of concerns, with a mean score of 5 and with the most threat categories listed in the set. The middle set of concerns consists of: Copyright Infringement of Electronic Archival Material, Data Breach from Library Computers and Servers, Personal Identification Theft Associated Library Accounts, Man-in-the-Middle Attack (people hijacking or listening in on the network), Network Listening Devices (library patrons), Unauthorized Access of Network from within the Library i.e., Wi-Fi Range Network and Equipment Tamper (computer, USB cords, fax machines, wall outlets, charging stations), Unauthorized Access of Library Network, Archival Digital Collection Protection from Corruption or Malicious Alteration.

Bottom Set of Concerns - The bottom concerns have a mean score of 4 and consist of Journal Database Theft, Digital Collection Theft, Personal Identification Theft associated with Archive Accounts, Personal Identification Theft associated with Library RFID (pretend you have one, if you do not), Personal Identification Theft associated with Archive Billing and/or Outside University Request.

Top 3 Sets

When examining standard deviations of each of these sets, it is important to take note of the following concepts. When a standard deviation is between 2 and 2.5, this indicates that 95 percent of the responses are within the mean score. When examining both Top Concern and Second Top Concern, their standard deviations fall between this 2 - 2.5 standard deviation range. Thus, the data scores collected from the group are close. This would indicate that most of the spread is “tight”, and general consensus and confidence of this score is high. In the Third Top Set, the standard deviation falls within the 2.5 - 3.0 range which is still considered a fairly tight cluster. One thing to note is that on the threat issue of Ransomware of Library Systems, the standard deviation has the most spread at 2.97 with a variance of 5.79 on a scale of 1-10. This is a very strong variance of opinions which is worth noting.

Middle Sets

When examining the Middle Set, the standard deviation ranges between 2.5 - 3.21. This indicates the spread from the mean is widening. Only one threat ranged outside the 3.0 range, Archival Digital Collection Protection from Corruption or Malicious Alteration. On the threat issue of Data Breach from Library Computers and Servers, survey participants were beginning to indicate a wider opinion with the standard deviation of 2.98.

Bottom Sets

The Bottom Sets have the largest standard deviation with variations. The standard deviation for the bottom ranges from 2.64 - 3.29 with a variation ranging from 7 - 10 on a 10-point scale. This indicates a significant difference in opinions on the threats listed in this group.

Q5 - Were you aware of these threats?

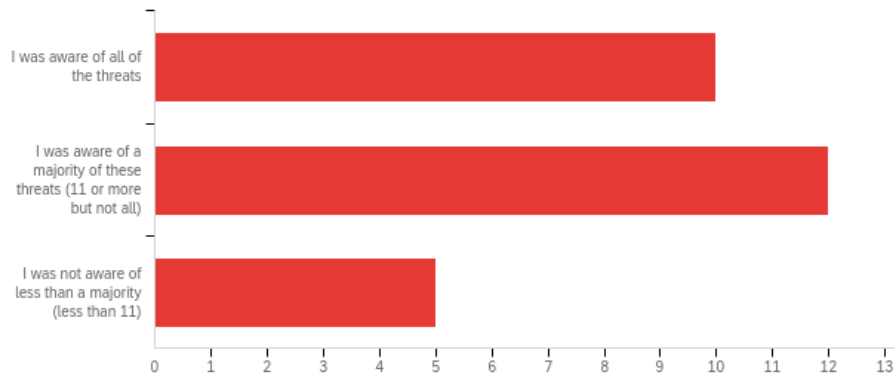


Figure 4: Cybersecurity Threat Awareness

Awareness reveals that 22 out of 27 participants are aware of the majority of the threats the library faces. This is a very good number, indicating that SL, CIT, and A are very knowledgeable and are concerned with cybersecurity. This could mean that if these participants were included in policy conversations, they may have an added value or opinion.

6.3 Analysis of Section 3: Direct Communication of Policy (4 Questions)

Q6 - How well do you feel that cybersecurity policy is communicated to your department?

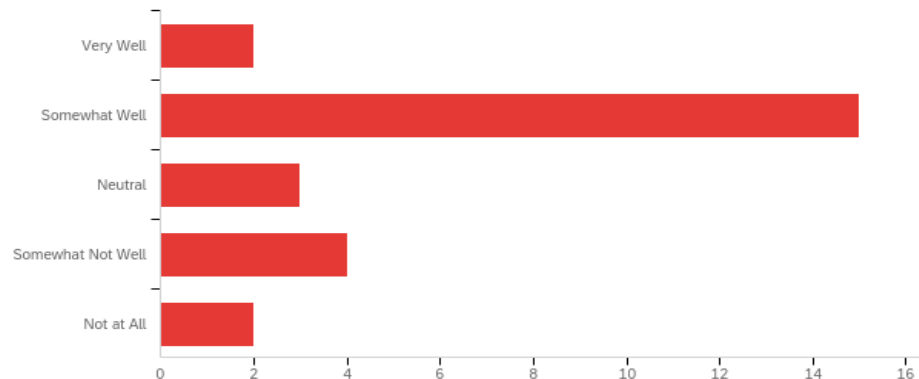


Figure 5: Cybersecurity Department Communication

Of the 26 persons surveyed, 17 indicated that they feel that communication of cybersecurity within the department is going well. A total of 9 participants responded neutrally, somewhat not well, or not at all well. Remember that 7 of the participants are UITS cybersecurity specialists. If those 7 particular participants are subtracted from the overall results, that would leave 10 out of the remaining 19 participants, only slightly more than half, who feel that cybersecurity is being communicated at least somewhat well.

Q7 - How familiar are you with all aspects of university cybersecurity policy?

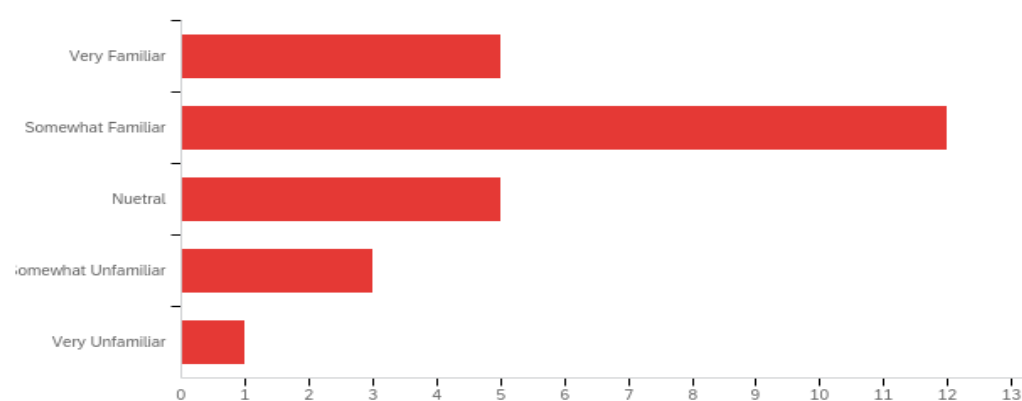


Figure 6: Cybersecurity University Policy Familiarization

Regarding the 26 participants, 9 reported that they were either neutral, somewhat unfamiliar, or very unfamiliar with university cybersecurity policy. Again, subtracting the 7 cybersecurity specialists out of the participants, the reconsidered result is 9 out of 19 respondents.

Conversely, this indicates that only slightly over 50 percent of librarians and archivists were familiar with university cybersecurity policy.

Q8 - How often do you review the policy for policy changes?

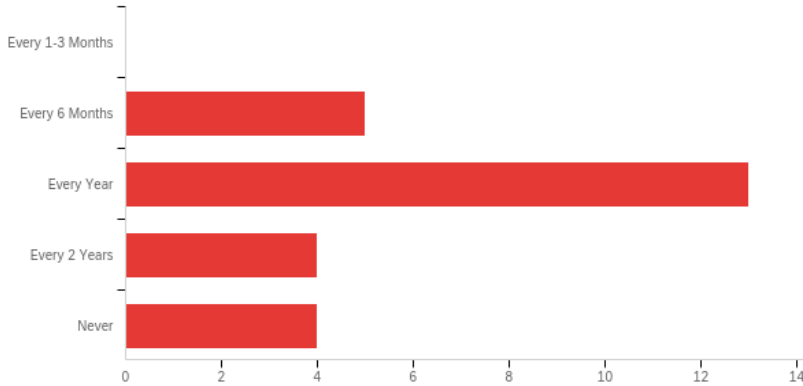


Figure 7: Cybersecurity Policy Review

The majority (13/26) of participants indicated that they review the university cybersecurity policy every year. Five more participants indicate reviewing every 6 months. This indicates that the majority of participants will dedicate some of their time to the review of cybersecurity policy, if it is available. However, there were still 4 participants who reported that they have never reviewed cybersecurity policy changes. This suggests that there is room for improvement.

Q9 - How are new policy changes communicated to you? (May Select Multiple Answers)

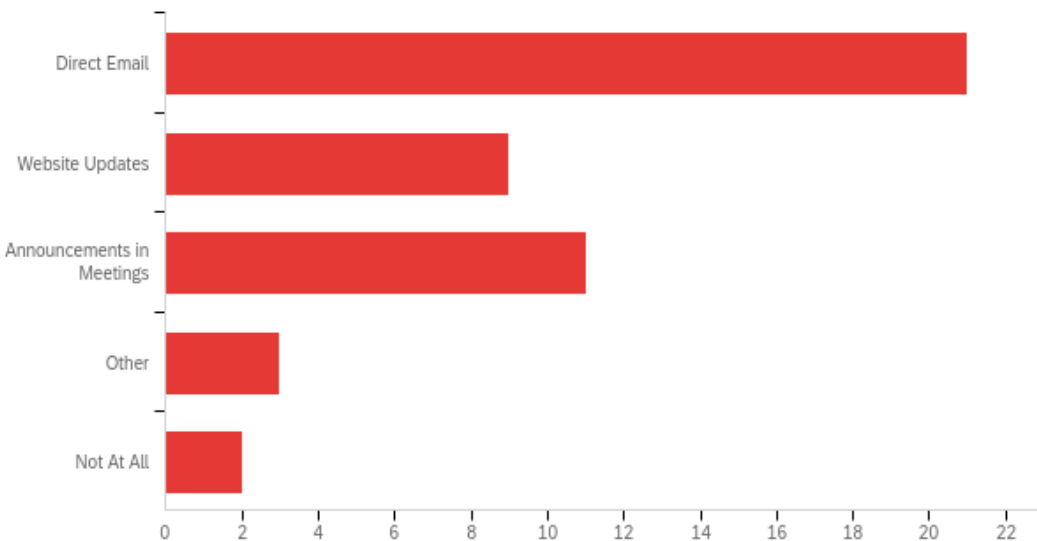


Figure 8: Cybersecurity Policy Communication after Changes

This question clarified that the vast majority of communication of policy comes from one of three sources: direct email, website updates, or meeting announcements.

6.4 Analysis of Section 4: Cybersecurity Policy Creation or Participation (3 Questions)

Q10 - I have been involved in creating cybersecurity policy for the library.

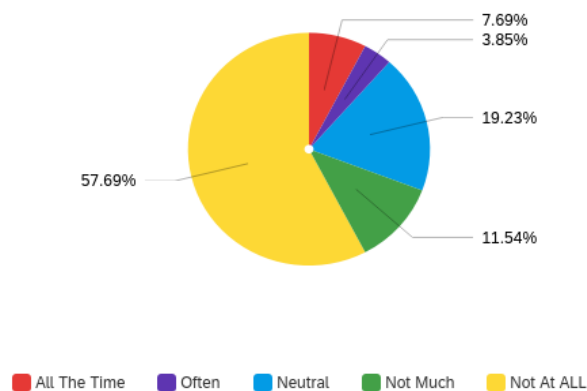


Figure 9: Cybersecurity Inclusion in Policy Creation

This chart indicates that 69.23 percent of respondents have not participated in library cybersecurity policy creation, and only 11.54 percent have or are involved in cybersecurity policy creation. More on this topic will be available in the survey conclusion section.

Q11 - Have you ever been asked to provide your opinion about university cybersecurity policy?

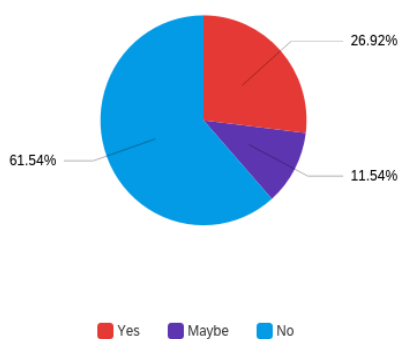


Figure 10: Cybersecurity Policy Inclusion

Only 26.92 percent of participants indicated that they have been asked an opinion on cybersecurity policy. This leaves 61.54 who have never been asked for their opinion.

Q12 - How often is library cybersecurity policy reviewed for changes or edits?

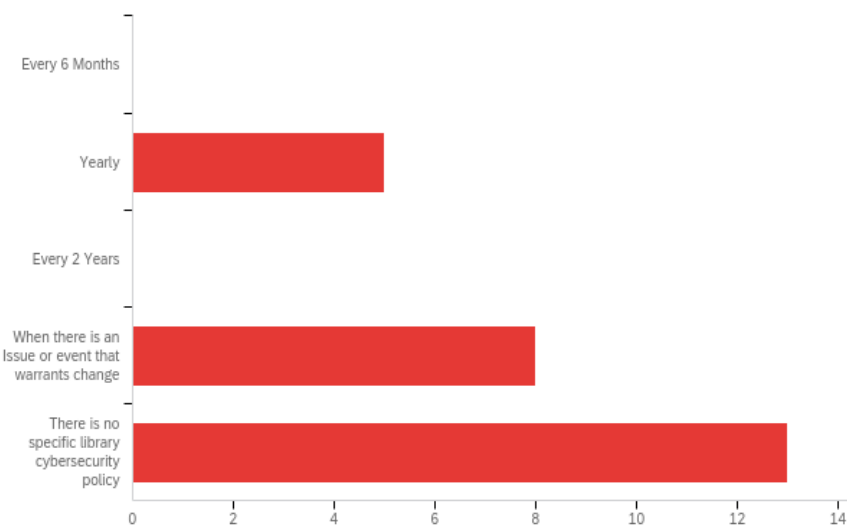


Figure 11: Cybersecurity Policy Review Frequency

21 of the participants indicated that they have no set schedule for library cybersecurity review or changes. This is an alarming finding that will be further discussed in the survey conclusion.

6.5 Analysis of Section 5: Reporting Procedures (4 Questions)

Q13 - Have you reported a cybersecurity issue or asked to resolve a cybersecurity issue or event?

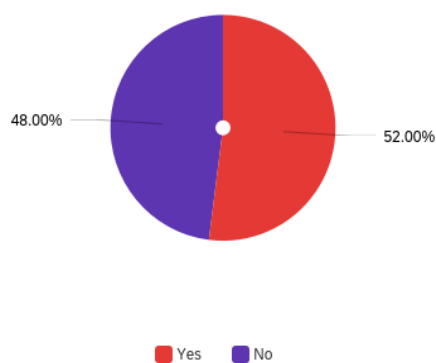


Figure 12: Cybersecurity Occurrence

52% of participants have either reported or been asked to resolve a cybersecurity issue. Even taking out the 7 CITs, this is a significant number (6/18) which is one-third of librarians or archivists who have witnessed a cybersecurity event.

Q14 - If Yes, was the result of the report ever communicated back to you or was a policy changed from UITS resulting from the report?

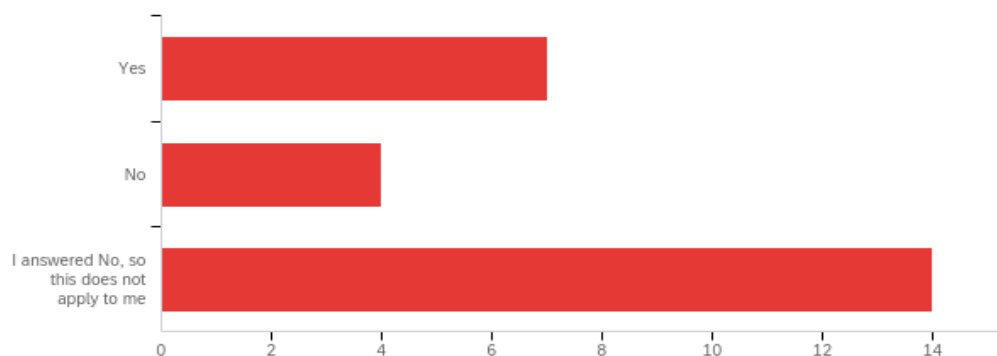


Figure 13: Report Feedback Loop

While this question does not apply to most of the participants, it is significant to note that four participants who reported an event did not receive any kind of report or indication of what happened to that event.

Q15 - Have you ever been shown any reports indicating threats or activities of possible threats?

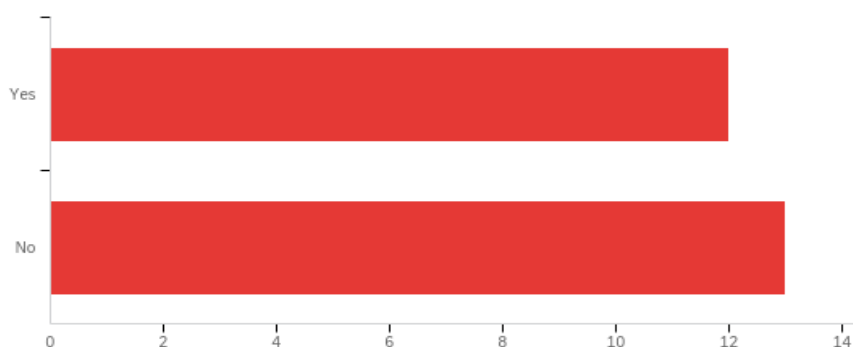


Figure 14: Cybersecurity Awareness of Possible Threats

Only 12 (48%) out of 25 participants have received reports indicating threats or possible threats.

Q16 - Are you ever given any indication of the health/quality/status of your cybersecurity efforts?

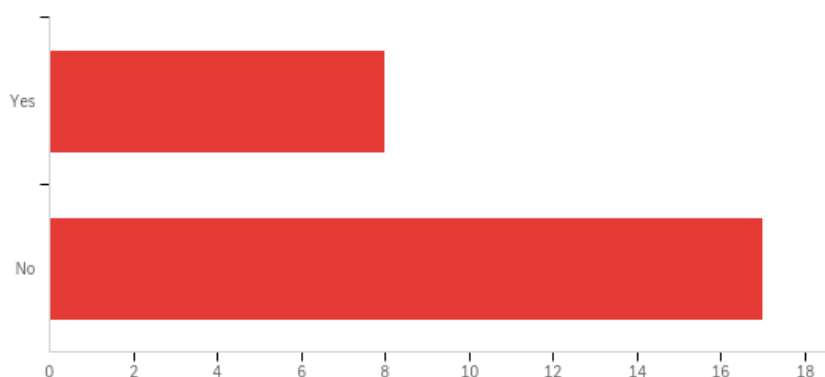


Figure 15: Network Health Status

Only 8 (32%) out of 25 participants indicated that they receive some kind of status or health report of cybersecurity efforts.

6.6 Analysis of Section 6: Things That Get Left Out (1 Question)

Q17 - Are you aware of any library or archive cybersecurity policies that are not included in university general cybersecurity policies (examples -- Thumb drive discovery of unknown owner that is screened for antivirus before inserted into computer to find its owner, or library cell phone cords checked for inserted hijacking or listening devices, etc.)? If yes, please give the name of policy and, if you could, the general gist of the policy.

Table 2: Cybersecurity Survey Comments

#	Direct Comments from the Survey
1	Yes, it falls in the policy of appropriate use.
2	Our library should have them or reference them in their Departmental Information Security Plan that they review each year and have everyone in the department sign.
3	At this time, I do not know of any outside policies for our library that do not directly come from the system-wide cybersecurity policies in place. We do not open abandoned thumb drives to find their owners' information (kept in a safe lock).
4	We do not open abandoned thumb drives to find their owners' information (kept in a safe location for 24 hours before taking them to lost and found).

5	We do not loan out charging cords. (We have one charging station directly across from our circulation desk).
6	No specific library policies beyond university policies; common-sense treatment of lost USB drives - not to be inserted into library computers.
7	As a whole, most of our online policies are less than to be desired. I do know ITS is actively reviewing and updating old policies.

Responses 1 and 6 indicate a lack of policy. Response 7 indicates need for policy improvement.

Responses 3 and 4 may indicate that this is just a procedural norm with no formal policy.

6.7 Analysis of Section 7: Overall Reflective Barometer (1 Question)

Q18 - How well do you feel that cybersecurity policy is communicated to your department on a scale 1-10, with 10 being that cybersecurity policies are communicated clearly through proper modes of delivery and with appropriate frequency?

The mean average for the group was 5.1 as indicated by Figure 16. Table 2 represents the barometer readings relating to each correspondence rating. Only 10 respondents rated communication of cybersecurity policy as a 7 or higher. While 11 of the respondents rated communication of policy as a 5 or lower.

Table 3: Barometer Rating Responses

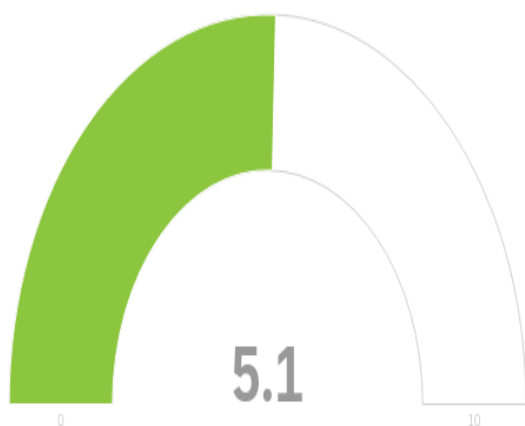


Figure 16: Cybersecurity Barometer

Field	Choice Count
0	4.76% 1
1	4.76% 1
2	4.76% 1
3	19.05% 4
4	14.29% 3
5	4.76% 1
6	0.00% 0
7	33.33% 7
8	4.76% 1
9	9.52% 2
10	0.00% 0
	21

Showing rows 1 - 12 of 12

6.8 Survey Improvement Considerations

Because the sample population consisted of 32 participants from 24 academic institutions, this sample population might be considered a small sample size. A recommendation for a greater number of participants and academic institutions could be made and, subsequently, compared to the results found in this paper. Additionally, some librarians, when contacted, had a problem with the term “system librarian”. This is because some academic institutions do not have a librarian who does only system librarian work. Some institutions are very integrated with university information systems. They may have a person from UITS designated to the library network. Perhaps the survey, next time, should just use the term librarians or University Information Technologies that would handle cybersecurity functions.

7.0 Survey Conclusion

Prioritization of cybersecurity threats vary widely among the following threats:

Table 4: Highest Variance Rates Amongst Cybersecurity Threats

Threat	Mean	Variance	Std
Personal Identification Theft Associated with Archive Accounts	4.4	11.52	3.39
Personal Identification Theft Associated with Archive Billing and/or Outside University Request	4.38	10.9	3.3
Digital Collection Theft	4.46	10.33	3.21
Archival Digital Collection Protection from Corruption or Malicious Alteration	5.0	10.32	3.21
Network Listening Devices (Library Patrons)	4.88	9.47	3.08
Equipment Tamper (computer, USB cords, fax machines, wall outlets, charging stations)	4.73	8.89	2.98
Data Breach from Library Computers and Servers	5.2	8.88	2.98
Ransomware of Library Systems	5.58	8.47	2.91

This particular set of threats is where Librarians, Archivists, and University Information Technologists begin to differ in opinion as to whether or where to spend resources (money, technology, time) to monitor or defend from cyber-attacks. Librarians and Archivists view these

threats as high priority, while University Information Technology Services view these threats as low priority. To compound this problem, the Tier 3 University System of Georgia Information Technical Service (USGITS) is more than likely in line with UITS and, also, views these threats as low priority. (Again, it would be beneficial to conduct another survey to compare this).

These particular threats are especially vulnerable to attacks, because the policy creation and provision of resources (money, technology, time) are dictated from the higher management tier 3, such as the USGITS. USGITS, more than likely, views these cybersecurity threats as a low priority, but Librarians and Archivists do not view these threats as a low priority.

The good news is that a majority (81.5%) of the participants are aware of the majority of the threats as interpreted from question 5. This would indicate that there is a good chance that if *SL*, *A*, and *CIT* work together on cybersecurity policy, then they would not get stuck so much on the definition or knowledge of these types of cybersecurity issues.

7.1 Cybersecurity Communication Gap

One of the problems is communication of cybersecurity policy which is identified multiple times in the survey. Question 6 demonstrates that 50% of the SL and A do not feel that cybersecurity is communicated well within the department. This question is nearly repeated in the barometer question (Q18) which allows the participants to gauge their feelings about cybersecurity communication. The results are 5.1 average on a 10-point scale barometer. Both question 6 and question 18 demonstrate that the majority of participants do not feel cybersecurity policy is being communicated clearly, appropriately, or frequently enough. Question 7 also demonstrates that, after factoring out UITS, 50 percent of the participants are only somewhat unfamiliar or totally unfamiliar with the university cybersecurity policies. When examining the results from questions 6, 7, and 18, the theme of communication of policy is becoming an issue at the

university level. The main point here is that if the staff members do not think communication is going well, then cybersecurity policy and implementation of new cybersecurity policy will not be as effective, potentially producing gaps or breakdowns in defense from cyber-attacks.

7.2 Cybersecurity Policy Inclusion and Creation

As cybersecurity policy pertains to creating, or participating in creating, cybersecurity on the university level, questions 10, 11, and 12 demonstrate a severe lack of cybersecurity policy creation or community. Question 10 indicates that 69.23 percent of respondents have not participated in library cybersecurity policy creation. Question 11 demonstrates 61.54 of participants have never been asked an opinion on cybersecurity policy. Question 12 reveals that 8 out of the 13 participants who actually have been involved with cybersecurity only make changes to policy after an event has occurred instead of on a cyclic basis. When examining these three questions (10, 11, and 12), a real lack of participation and added guidance of policy from *SL*, *A*, and *CIT* becomes apparent. The lack of participation leads to problems with enthusiasm, improved protection, and community engagement. How can improvement be expected in this environment when the answer is that policy is only changed when an event happens? How can community involvement be built when the answer to how often cybersecurity policy is reviewed is 2 years to never (question 8)? In resolving the communication issue of cybersecurity policy, community involvement must be in the solution.

7.3 Cybersecurity Reporting and Feedback

Reporting is a major part of cybersecurity policy; questions 13, 14, 15, and 16 probe into this issue. Table 5 is data gathered from the survey and parsed out according to Librarians and Archivists.

Table 5: Reporting/Feedback/Status Reports

<i>Q13 - Have you reported a cybersecurity issue or asked to resolve a cybersecurity issue or event?</i>		
	Reported Cybersecurity Event or Issue	Never Reported Cybersecurity Event or Issue
Librarians & Archivists	8/26 (30.76%)	12/26 (46.15%)
Cybersecurity Information Technologists	7/7 (100%)	
<i>Q14 - If Yes, was the result of the report ever communicated back to you or was a policy changed from UITS resulting from the report?</i>		
	Yes, report communicated back	No, report was not communicated back
Librarians & Archivists	6/8 (75%)	2/8 (25%)
Cybersecurity Information Technologists	4/7 (57.14%)	3/7 (42.86%)
<i>Q15 - Have you ever been shown any reports indicating threats or activities of possible threats?</i>		
	Shown report	Not shown a report
Librarians & Archivists	13/26 (50%)	13/26 (50%)
Cybersecurity Information Technologists	7/7 (100%)	
<i>Q16 - Are you ever given any indication of the health/quality/status of your cybersecurity efforts?</i>		
	Yes	No
Librarians & Archivists	11/26 (16.27%)	15/26 (57.69%)
Cybersecurity Information Technologists	5/7 (71.43)	2/7 (28.57%)

An interesting finding is that 52 % (13/25) of all participants had reported a cybersecurity event. Moreover, almost 31 % of the 52 % are Librarians and Archivists. Noteworthy, is that 100 % of the Cybersecurity Information Technologists have reported a cybersecurity event. The main takeaway point is that Librarians and Archivists are facing cybersecurity issues on the ground level and are, subsequently, attempting to report these events. In question 14 findings, 75% of Librarians and Archivists of events reported resulted in a cybersecurity policy change with notification to the reportees that a policy had occurred. This means that 25% of the reported

cases have no communication or response that anything has been done with their reported incident (not factoring in UITS personnel). This could lead to discouraging reporting behaviors; for instance, if those who report do not believe that anything is going to be done or that their report is pointless, then why report it in the first place? Again, a communication plan would include a feedback loop so that reports filed are closed with a response from the cybersecurity team. The report filed from the cybersecurity team needs to detail what actions were or were not taken and/or their recommendations. Along these same lines are the question 15 findings which indicate that only 50 percent of Librarians and Archivists have ever seen a threat/incident-type report. That is compared to 100% of Cybersecurity Information Technology Specialists. This means that the university cybersecurity professionals have the information but, for some reason, do not think it is important to pass it on to the departments within the university. Question 16 is similar to question 15 in that participants are asked if they are given any indication of the health status of the network. A similar percentage, 57.69 percent of Librarians and Archivists, had not received any kind of health status on their network. As part of the communication loop, it is essential for cybersecurity professionals to let the community they protect and serve know what is happening in cyberspace. This, in turn, increases vigilance and reporting efforts.

7.4 Policy Improvement

Nothing noticeable appears at first glance of the responses to the open-ended question 17. However, upon closer examination, two responses suggest policy improvement and two responses suggest policy omission. If higher education libraries are expected to protect patrons and be protected from cybersecurity threats, such as ransomware and malware prioritized in the Third Set Figure 17, a policy regarding lost-and-found thumb drives and electronic devices needs to be clearly defined.

7.5 Summary Recap

A difference of prioritization of cybersecurity threats occurs between Librarians, Archivists, and Information Technology Professionals. This may lead to policy omissions or incomplete cybersecurity policies. Additionally, while not examined in this survey, this may also lead to resource allocations deficits by prioritizing what those who occupy Tier 3 think are the most important cybersecurity issues. A communication gap or disconnect exists when considering the cybersecurity needs of those who occupy Tier 1 (Librarians and Archivists). This is shown in the survey when examining inclusion and policy creation. While not succinctly proven by this survey, although signs of such are noticeable, enthusiasm or lack thereof could contribute to this problem, because, perhaps, Librarians and Archivists do not feel like they are a part of the cybersecurity efforts. A severe issue with the reporting loop is apparent; many of the participants are not receiving information on current cybersecurity threats and the health of the network. Again, this could lead to Librarians and Archivists not feeling part of the cybersecurity defense, creating a possible lack of enthusiasm. Of note are the comments in question 17 that read:

“As a whole, most of our online policies are less than to be desired. I do know ITS is actively reviewing and updating old policies.”

This indicates that Librarians and Archivists are not satisfied with the current state of cybersecurity policies in their institutions. A barometer reading of 5.1 from System Librarians and a 3.5 from Archivists indicates that communication of cybersecurity policy is weak in aspects of clarity, modes of delivery, and appropriate frequency (as seen in Figure 17).

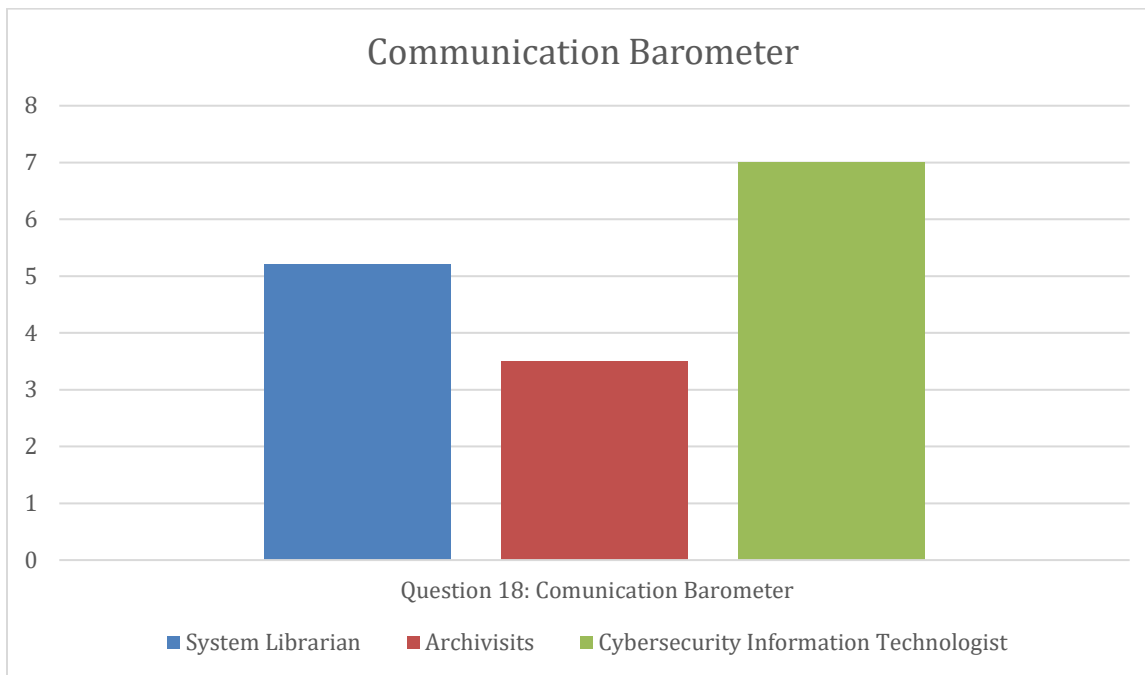


Figure 17: Communication Barometer

The average score for the communication of cybersecurity information technologist is 7, indicating this group believes that communication of the cybersecurity policy in terms of clarity, frequency and mode is above average. A distinct difference in opinion on how each group views the communication issues is noticeable. In order to bring these scores closer to alignment, a different approach to community engagement might be helpful.

8.0 Proposed Policy Solution of Communication Enlightenment Engagement Plan (CEEP)

One possible solution is a Communication Enlightenment Engagement Plan (CEEP) which connects the issues of communication, engagement, and status as they pertain to cybersecurity issues, events, and policy among Tier 1 (USGITS), with Tier 3 (Librarians/Archivists departments), and involves Tier 2 (UITs).

CEEP would have a policy creation and review mechanism as shown in Figure 18.

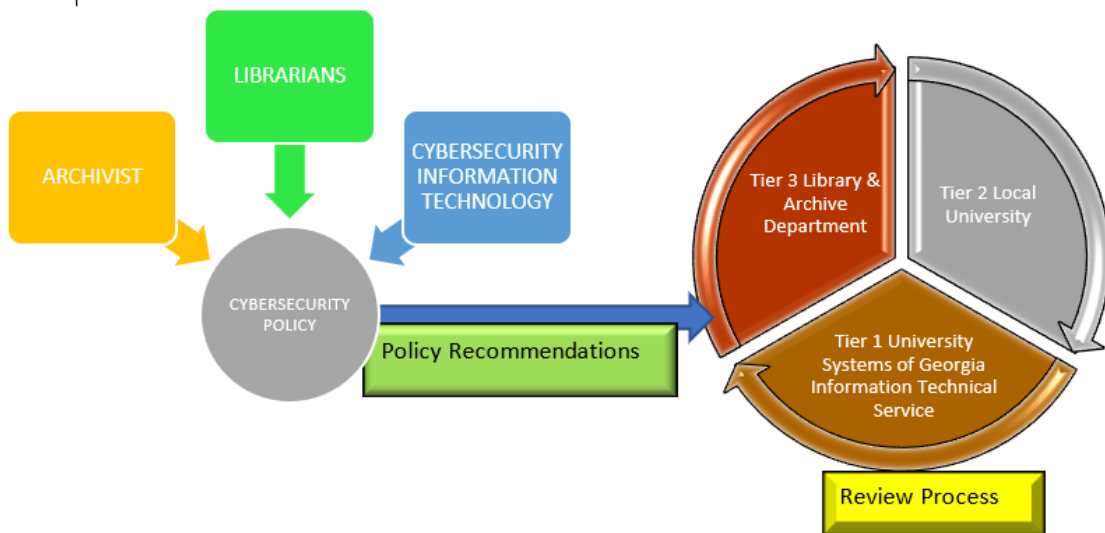


Figure 18: CEEP Conceptual Model

This process would increase awareness, participation, and inclusion with cybersecurity policy. Sometimes, cooperation is pertinent to implementation and buy-in (following policy) as it relates to success in security measures. Additionally, if cybersecurity leaders and/or defenders of cybersecurity policy are available within the departments in which the policy governs, the department is more likely to follow policy. Thus, this creates a feeling of cybersecurity awareness. This has a high potential of an increased cybersecurity barometer recording; in which case, a future survey could be done from the baseline reading collected from this survey. (In other words: somebody might consider doing a study on this point.)

CEEP needs a report feedback loop between all tiers (1, 2, and 3).



Figure 19: Report Feedback Loop

The blue represents Tier 3; the yellow, Tier 2; and the green, Tier 1. A report filed in Tier 3 (Library/Archives) is received by both Tier 2 (UITS) and Tier 1 (USGITS). Tier 2 begins to resolve the issue and, eventually, reports back to Tier 1. Tier 3 might be brought into the resolve process, depending on the issue. Now, of course, this is an oversimplification of the process. The point is: some kind of communication needs to take place between the tiers in order for those occupying Tier 3 to know what the issue was and how this issue is being addressed instead of going into some kind of a void. Tier 1 needs to have documentation of the events that are being addressed at the lower levels in order to make policy decisions concerning departments. This also helps with the cybersecurity review and policy creation process, as shown in Figure 18. When Tier 3 makes a recommendation, and it passes through to Tier 2, Tier 3 may reference events that took place leading to the policy recommendation, and Tier 1 would have the documentation supporting the changes being recommended.

A CEEP would mitigate the risk of the cybersecurity issues stated above. The title CEEP is used instead of Cybersecurity Communication Plan, because the latter often pertains to crisis management and response. I would like to extend that to include communication of policy, reporting of events, reporting of solutions, reporting the status of attacks, and inclusion of policy

creation. Many academic institutions dictate policy from top tiers of governance down to the university level. As seen from this survey, certain departments are excluded from policy creation and reporting. Enterprise Architecture has demonstrated in larger organizations a need to have both inclusion and communication of policies between departments in order to be effective, especially during a time of crisis. More importantly, specific issues and concerns that both Librarians and Archivists deal with do not fit neatly into general all-encompassing top tier university information systems technology policy. This leads to security gaps that could be exploited, because no one has even considered or been consulted. These circumstances might lead to the next academic cybersecurity breach.

9.0 Conclusion

The survey recap section points to compelling evidence of a communication gap between tiers, a lack of inclusion in policy creation, and no feedback loop when reporting events. These three issues contribute to a feeling of an inferior cybersecurity policy. As prioritizing threats, a strong agreement among the top 2 tiers of threats exists; however, once an observer examines the Third Set of threats, a large variance of agreement becomes apparent. This has an impact on where money and resource allocations will be distributed when deciding cybersecurity defense. Money allocation also affects cybersecurity policy or the effectiveness of the policy. While this survey did not review the direct effects of the morale barometer (Survey Question 18) on reporting and carrying out policy, an argument could be made if the departments do not feel their efforts are being acknowledged or are left out of the policy creation, then this could lead to poor reporting efforts.

The results from the survey indicate that a top-down approach has resulted in communication issues. Although this author has offered CEEP as one possible solution, which is both bottom-up

feedback with a top-down governance approach, more alternatives could be explored. However, the way the policy is created, communicated, and reviewed seems to lead to a poor barometer of cybersecurity policy in current USG institutions. This result could lead to poor cybersecurity defense which could be remedied by simple inclusion of input in policy creation and review from the end department.

References

- Ajie, I. (2019). A Review of Trends and Issues of Cybersecurity in Academic Libraries. *Library Philosophy and Practice*, 1-20.
- American Library Association, (2016, August 24). Keeping Up With... Cybersecurity, Usability, and Privacy. [webpage]. *American Library Association*. Retrieved on April 24, 2020 from http://www.ala.org/acrl/publications/keeping_up_with/cybersecurity. Document ID: 243e4b00-03fe-c544-2150-3f2cd22cedc7
- American Library Association. (2017, May 29). Academic Freedom. [online]. *American Library Association*. Retrieved on 04/19/2020 from <http://www.ala.org/advocacy/intfreedom/>.
- Bates, C., Bowen, A., Morton, M., Washington, C. (2019) Campus cybersecurity teams face a broad range of challenges today. [video] *Higher Education Information Security Council*. Retrieved on 04/20/2020 from <https://library.educause.edu/topics/cybersecurity>.
- Board of Regents of the University of Georgia. (2020). University of Georgia: *USG information Technology Handbook*. Board of Regents of the University of Georgia. Retrieved from https://www.usg.edu/assets/information_technology_services/documents/2020_IT_Handbook.pdf.
- Hennig, N. (2018). *Privacy and Security Online: Best Practices for Cybersecurity*. ALA TechSource, American Library Association.
- Indiana University Council of Head Librarians. (2012). Indiana University Libraries Privacy Policy. [Webpage] *Indiana University Council of Head Librarians*. Retrieved from <https://policies.iu.edu/policies/lib-01-libraries-privacy/index.html>.
- Landgraf, G. (2018). Data Collection and Privacy: Balancing information needs with patron protection. *American Libraries*, 49(9/10/2018), 14–15.
- National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology*. Retrieved on 04/21/2020 from <https://colstate.view.usg.edu/content/enforced/1967511-CO.300.CSMT6222.24140.20204/NIST.CSWP.04162018.pdf>.
- Nicolas-Rocca, T. S., & Burkhard, R. J. (2019). Information Security in Libraries: Examining the Effects of Knowledge Transfer. *Information Technology and Libraries*, 38(2), 58.
- Rudasill, L., & Moyer, J. (2004). Cyber-security, cyber-attack, and the development of governmental response: the librarian's view. *New library world*.
- Smith, F. A. (2017). Should Libraries Even Consider Hacking Back If Attacked/ /Felicia A. Smith. *Computers in Libraries*, 37, 14-16.
- University System of Georgia. (2020). Providing trusted premier solutions to advance the University of Georgia higher education enterprise. [webpage] *Information Technology Services*. Retrieved from https://www.usg.edu/information_technology_services/.

Appendices

APPENDIX A: Columbus State University Policy Review & NIST

27 UITs Information Security Policies Found at

https://infosec.columbusstate.edu/securitypolicies/security_policies.php

Access Control Policy

https://infosec.columbusstate.edu/securitypolicies/user_access_control_policy.pdf

By Paul Luft

Policy Review Continued on Next Page

NO.	CONTROL	YES	NO	NOTES
<u>AC-1</u>	ACCESS CONTROL POLICY AND PROCEDURES	X		Some things are still vague here. There is no scope subsection which is sort of listed in Purpose. Coordination is somewhat there (Banner, HR, Students).
<u>AC-2</u>	ACCOUNT MANAGEMENT	X		This does define Account Managers.
<u>AC-3</u>	ACCESS ENFORCEMENT	X		This, to me, comes in the form of the Login Policy and Password Policy. There are control enhancements that I feel would be an improvement. As stated in the Login Policy, biometrics and duo authentication is not allowed.
<u>AC-4</u>	INFORMATION FLOW ENFORCEMENT	X		States that access is granted according to duties. This is done to protect duties. This might be considered an Enhanced feature of AC-3(7).
<u>AC-5</u>	SEPARATION OF DUTIES	X		I feel this is covered in Network ID Policy to define responsibilities of users.
<u>AC-6</u>	LEAST PRIVILEGE	X		This is, definitely, covered in Network ID Policy. This has some enhanced features such as review of policies (AC-6). Also, special circumstances are mentioned in Network Policy.
<u>AC-7</u>	UNSUCCESSFUL LOGON ATTEMPTS	X		This information is stated in the CSU Password Policy. Also, enhanced control measures are mentioned on mobile devices in Portable Devices Policy.
<u>AC-8</u>	SYSTEM USE NOTIFICATION	X		This does display One USG authentication. This one, to me, is kind of hard to find within all the policies. There is a little bit located in the Appropriate Information Use Policy that explains that we comply with state and laws. I am going to say, yes, it is covered here.

AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION	X		This is covered under Log Maintenance Policy.
AC-10	CONCURRENT SESSION CONTROL		X?	I could not find this mentioned in the 27 policies. I know when I'm working in my office and then walk out to the reference desk, if I have email open in both places, a message does appear that asks if I want to terminate connection (or something to that extent). This leads me to believe there is a policy, but I'm not able to find it within these documents, yet.
AC-11	SESSION LOCK		X	The Log Maintenance Policy has a bullet point about start up and shut down. It really does not talk about session lock. Network Policy does not talk about session lock. This is sort of covered in Appropriate User Policy.
AC-12	SESSION TERMINATION		X	I'm really having a hard time finding this one, as well. It is, also, somewhat, covered in Appropriate User Policy.
AC-13	SUPERVISION AND REVIEW - ACCESS CONTROL	X		Yes, this is, definitely, mentioned in User Access Policy.
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	X		Network User ID Policy does state that non-student IDs can be obtained for specific circumstances. (We do this in the library for public patrons.)
AC-15	AUTOMATED MARKING	X		There is not much stated here.
AC-16	SECURITY ATTRIBUTES	X		I feel this is located in different Policies: Appropriate Use Policy – Privacy Protections, Network User ID with access privileges to certain materials/database/information and Portable Device Policy with limiting access controls.
AC-17	REMOTE ACCESS	X		There is, specifically, a policy on Remote Access Policy which also contains VPN agreement, amongst other things.
AC-18	WIRELESS ACCESS		X	I don't feel the Portable Access Policy covers wireless access.
AC-19	ACCESS CONTROL FOR MOBILE DEVICES		X	I don't feel the Portable Access Policy covers wireless access.
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	X		Both Remote Access and Portable Device Policies cover this.
AC-21	INFORMATION SHARING	X		FERPA - Appropriate Information Policy

AC-22	PUBLICLY ACCESSIBLE CONTENT	X		Most of this is in Data Privacy Policy & Appropriate Information Policy.
AC-23	DATA MINING PROTECTION	X		Most of this is in Data Privacy Policy & Appropriate Information Policy.
AC-24	ACCESS CONTROL DECISIONS	X		I feel like this is, sort of, been covered but Network User ID Policy.
AC-25	REFERENCE MONITOR	X		Log Maintenance Policy

Summary Report

Review of 27 Information Security Policies at Columbus State University, Columbus, GA, were paired with NIST standards found at <https://nvd.nist.gov/>. The 5 controls that are either deficient or missing (will be further explained) are [AC-10](#), [AC-11](#), [AC-12](#), [AC-18](#), and [AC-19](#). 20 Twenty controls were found in accordance to NIST STANDARDS.

AC-10: States that a limit to concurrent session should be assigned to an account. Nothing seems to be stated within any policy as to how many sessions a user can have open. A test of the control can be conducted, and an employee of the Columbus State University (i.e., this writer) has experienced a message that warns that another session is open, when utilizing another device. While that may be what happens, there is not a stated policy that was found to say how many sessions could be open at one time within the 27 policies listed.

AC-11: Session lock was not found within the policy (see AC-12).

AC-12: This reviewer could not find anything about session timeout or termination of session. Testing the computer on the network does reveal that at some point in time relogging on to the network is required. Additionally, certain applications or systems, such as the learning management system, does have a timeout that is sooner than network session termination. Additionally, library databases or third-party applications may also have a timeout feature which happens through a proxy server. As far as an official policy, this reviewer could not find that out from policies reviewed.

Solutions

AC-10 – AC-12 have the same remedy: write a policy pertaining to what is actually being practiced on the site. The safeguards of session termination and concurrent session are being executed by the network but are not found in policy. I would recommend stating, within these policies, the maximum time a session should be terminated based on the One USG login. The reasoning behind this is that all other applications seem to terminate before this time frame.

As for the concurrent sessions, this is a little harder to determine. This is where a discussion with network IT administrators, cybersecurity IT, and instructors needs to happen. This will need to be determined by the “load” the network can handle versus productivity and lifestyle of the students. The overall goal is not to limit access to one device at a time in an education setting.

Concurrent User Policy Resources for Remedies

<https://www.ibm.com/support/pages/what-does-concurrent-session-mean>

https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.0/com.ibm.isam.doc/wrp_config/concept/con_max_concu_sess_plcy.html

AC-18 and AC-19 have several issues in meeting the NIST standards regarding the controls in place for remote and wireless security policies. AC-18 talks about mutual authentication. AC-19 has statements of virus scans and individual battery resources. Additionally, there are a good number of control enhancements that would be very beneficial in a wireless security policy, such as monitoring unauthorized connections and disabling wireless networking. This reviewer recognizes the fact that there is a statement about devices being registered, but it is not, it seems, logical to be able to find this information in a wireless security policy. What good is a policy about wireless devices if it is located in some obscure location?

Side note: This reviewer has talked to a UITs staff in the library about hubs and wireless security and has learned that residential students do have router signal limitations. I just do not know if that is campus-wide and where exactly that policy is located.

Recommendation for AC-18 & AC-19: Craft a policy for wireless and mobile devices.

Resources

IBM. (n.d.). What does concurrent session mean? [webpage] *IBM*. Retrieved from <https://www.ibm.com/support/pages/what-does-concurrent-session-mean>.

IBM. (n.d.). maximum Concurrent Session Policy. [Webpage] *IBM Knowledgebase*. Retrieved from https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.0/com.ibm.isam.doc/wrp_config/concept/con_max_concu_sess_plcy.html

Appendix B - Library Cybersecurity Communication Survey

(Word Document Print (Defers Slightly When Printed out in Word Document Format))

Survey Flow

Standard: Informed Consent (1 Question)

Block: Section 1: Background Information (2 Questions) (2 Questions)

Standard: Section 2: Prioritizing Cybersecurity Threats (2 Questions)

Standard: Section 3: Direct Communication of Policy (4 Questions)

Standard: Section 4: Cybersecurity Policy Creation or Participation (3 Questions)

Standard: Section 5: Reporting Procedures (4 Questions)

Standard: Section 6: Things that get left out (1 Question)

Standard: Section 7: Overall Reflective Barometer (1 Question)

Page Break

Start of Block: Informed Consent

You are being asked to participate in a research project conducted by Paul Luft, a student in the Masters of Cybersecurity Management program at Columbus State University. [If this project is student-led, provide the name of the faculty member supervising the study: Dr. Lydia Ray.]

I. Purpose: The purpose of this project is to provide information pertaining to a thesis involving communication gaps between librarians, University Information Technology Systems Services (UITS), and the archivist.

II. Procedures: A survey will be presented to the system librarians, UITS, and archivist. The survey will be no more than 20 questions and should not take more than one hour to complete. There will be no use of this data for other studies or any future use for research.

III. Possible Risks or Discomforts: No risk is expected other than possible nervousness when answering the survey questions. This can be alleviated by the option to not answer a particular question, if persons feel uncomfortable about answering. All information will be anonymous.

IV. Potential Benefits: It is expected that benefits from completing this survey will lead to enhanced cybersecurity policies and cooperation between departments.

V. Costs and Compensation: No compensation will be provided to the participants.

VI. Confidentiality: Data and survey will be confidential. Master Student will only be able to access data through Qualtrics (an online survey software) which will not identify individuals taking the survey. The data, itself, will be published but with no trace as to the participant who answered the questions. All data entered by the participants will be encrypted by Qualtrics by default. The Qualtrics survey settings will be modified so that the survey will NOT collect the IP addresses of the participants. The Qualtrics survey software is associated with the CSU account and, hence, is protected by this Master Student's password. The Qualtrics data may be downloaded to an excel sheet for further analysis by Master Student researcher. The laptop has

password protection. Only Master Student will have access to the excel sheet. The excel sheet and Qualtrics data will be deleted within one year of project completion.

VII. Withdrawal: Your participation in this research study is voluntary. You may withdraw from the study at any time, and your withdrawal will not involve penalty or loss of benefits.

For additional information about this research project, you may contact the Principal Investigator, Paul J. Luft, at 706-507-8641, or at luft_paul@columbusstate.edu. If you have questions about your rights as a research participant, you may contact Columbus State University Institutional Review Board at irb@columbusstate.edu.

I have read this informed consent form. If I had any questions, they have been answered. By selecting the I agree radial and Submit, I agree to participate in this research project.

- I agree (1)
- I disagree (2)

Skip To: End of Survey If You are being asked to participate in a research project conducted by Paul Luft, a student in the... = I disagree

End of Block: Informed Consent

Start of Block: Section 1: Background Information (2 Questions)

Q1 Please identify which of the following group you belong to:

- UITS, (1)
- Systems Librarian, (2)
- Archivist (3)

Q2 Please list University (Optional)

End of Block: Section 1: Background Information (2 Questions)

Start of Block: Section 2: Prioritizing Cybersecurity Threats (2 Questions)

Q4 Rank the following cybersecurity concerns as according to priority, with 0 being the lowest concern and 10 being the highest concern:

High Priority: A cybersecurity threat that you perceive will likely happen, causing severe issues with workflow and privacy AND no matter what little budget you have, you would put money toward combating the threat.

Medium Priority: A cybersecurity threat that you perceive may happen with consequence to workflow and privacy AND are willing to put some money on a limited budget toward combating the threat.

Low Priority: A cybersecurity threat that is unlikely to happen but still might have consequences to workflow and privacy AND you would only put money toward combating the threat if you had extra money to do so.

0 1 2 3 4 5 6 7 8 9 10

Ransomware of library systems ()

Unauthorized access of library network ()

Unauthorized access of network from within the library. I.e. Wi-Fi range network ()

Password Protection of library systems ()

Malware on library patron computers ()

Malware from lost & found personal devices such as USB ()

Data Breach from library computers and servers ()

Copyright Infringement of journal databases/thesis/research ()

Copyright infringement of electronic archival material ()

Journal Database theft ()

Digital Collection theft ()

Personal Identification theft associated with university network ()

Personal Identification theft associated with library Wi-Fi ()

Personal Identification theft associated with Library RFID (pretend you have one, if you don't) ()

Personal Identification theft associated Library Accounts ()

Personal Identification theft associated with Archive Accounts ()

Personal Identification theft associated with archive billing and/or outside university request ()

Email phishing attacks (Students and Staff) ()

Man-in-the-Middle Attack (People hijacking or listening in on the network) ()

Network Listening Devices (Library patrons) ()

Equipment Tamper (computer, USB cords, fax machines, wall outlets, charging stations) ()

Archival digital collection protection from corruption or malicious alteration ()

Q5 2. Were you aware of these threats?

- I was aware of all of the threats (4)
- I was aware of a majority of these threats (11 or more but not all) (5)
- I was not aware of less than a majority (less than 11) (6)

End of Block: Section 2: Prioritizing Cybersecurity Threats (2 Questions)

Start of Block: Section 3: Direct Communication of Policy (4 Questions)

Q6 How well do you feel that cybersecurity policy is communicated to your department?

Very Well (1) Somewhat Well (2) Neutral (3) Somewhat Not Well (4) Not at All (5)

How well do you feel that cybersecurity policy is communicated to your department? (1)

Q7 How familiar are you with all aspects of university cybersecurity policy?

Very Familiar (1) Somewhat Familiar (2) Neutral (3) Somewhat Unfamiliar (4) Very Unfamiliar (5)

How familiar are you with all aspects of university cybersecurity policy (1)

Q8 3. How often do you review the policy for policy changes?

- Every 1-3 Months (1)
- Every 6 Months (2)
- Every Year (3)

End of Block: Section 4: Cybersecurity Policy Creation or Participation (3 Questions)

Start of Block: Section 5: Reporting Procedures (4 Questions)

Q13 Have you reported a cybersecurity issue or asked to resolve a cybersecurity issue or event?

- Yes (1)
- No (2)

Q14 If Yes, was the result of report ever communicated back to you or was a policy changed from UITS resulting from the report?

- Yes (1)
- No (2)
- I answered No, so this does not apply to me (3)

Q15 Have you ever been shown any reports indicating threats or activities of possible threats?

- Yes (1)
- No (2)

Q16 Are you ever given any indication of the health/quality/status of your cybersecurity efforts?

- Yes (1)
- No (2)

End of Block: Section 5: Reporting Procedures (4 Questions)

Start of Block: Section 6: Things that get left out (1 Question)

Q17 Are you aware of any library or archive cybersecurity policies that are not included in university general cybersecurity policies (examples -- Thumb drive discovery of unknown owner that is screened for antivirus before inserted into computer to find its owner, or library cell phone cords checked for inserted hijacking or listening devices, etc.) If yes, please give the name of policy and, if you could, the general gist of the policy.

End of Block: Section 6: Things that get left out (1 Question)

Start of Block: Section 7: Overall Reflective Barometer

Q18 How well do you feel that cybersecurity policy is communicated to your department on a scale 1-10, with 10 being that cybersecurity policies are communicated clearly through proper modes of delivery and with appropriate frequency.

End of Block: Section 7: Overall Reflective Barometer

Appendix C - Question 4 - Raw Data

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Ransomware of library systems	1	10	5.58	2.91	8.47	26
2	Unauthorized access of library network	0	10	5.19	2.72	7.39	26
3	Unauthorized access of network from within the library. I.e. Wi-Fi range network	0	10	4.81	2.77	7.69	26
4	Password Protection of library systems	0	10	5.96	2.46	6.04	27
5	Malware on library patron computers	1	10	6.31	2.57	6.6	26
6	Malware from lost & found personal devices such as USB	1	10	5.54	2.79	7.79	26
7	Data Breach from library computers and servers	1	10	5.2	2.98	8.88	25
8	Copyright Infringement of journal databases/thesis/research	1	10	5.54	2.41	5.79	26
9	Copyright infringement of electronic archival material	1	10	5.23	2.68	7.18	26
10	Journal Database theft	0	10	4.31	2.64	6.98	26
11	Digital Collection theft	0	10	4.46	3.21	10.33	26
12	Personal Identification theft associated with university network	1	10	6.76	2.39	5.7	25
13	Personal Identification theft associated with library Wi-Fi	1	10	5.76	2.83	8.02	25
14	Personal Identification theft associated with Library RFID (pretend you have one, if you donate)	1	10	4.48	2.61	6.81	25
15	Personal Identification theft associated Library Accounts	1	10	5.27	2.75	7.58	26
16	Personal Identification theft associated with Archive Accounts	0	10	4.4	3.39	11.52	25
17	Personal Identification theft associated with archive billing and/or outside university request	0	10	4.38	3.3	10.9	24
18	Email phishing attacks (Students and Staff)	1	10	7.81	2.39	5.69	26
19	Man-in-the-Middle Attack (People hijacking or listening in on the network)	1	10	5.24	2.53	6.42	25
20	Network Listening Devices (Library patrons)	0	10	4.88	3.08	9.47	25
21	Equipment Tamper (computer, USB cords, fax machines, wall outlets, charging stations)	0	10	4.73	2.98	8.89	26
22	Archival digital collection protection from corruption or malicious alteration	0	10	5	3.21	10.32	25