The purpose of this paper is to study and recommend directions for future research.

The methodology section also describes data collection and analysis techniques. Third, the findings are interpreted. The paper concludes with a discussion and explication of implications of the study and recommends directions for future research.

Keywords
Security; Trustworthy Digital Repositories; Repository Staff Perceptions.

1. INTRODUCTION
Unusually, security is part of what is necessary for a digital repository to be trustworthy. Evidence of the importance of security can be seen by examining criteria pertaining to security as part of recent standards for Trustworthy Digital Repositories (TDRs). For example, criterion C34 requires staff at organizations to protect the integrity of repositories and their contents [4, 11]. In particular, criterion C34 requires staff at organizations to protect the integrity of repositories and their content. To accomplish this, the security documentation for TDRs includes specific criteria pertaining to security as part of recent standards for Trustworthy Digital Repositories.

2. SCHOLARSHIP ON SECURITY
2.1 Security in the Digital Preservation Literature
Security refers to “the practice of defending information from unauthorized access, use, disclosure, disruption, modification, denial of service, recording or destruction” [16, p. 224]. The best place to understand the phenomenon of security within the field of digital preservation is to examine recent standards for TDRs. They represent a consensus among key members of the digital preservation community on what constitutes best practice. They include specific criteria pertaining to security as part of recent standards for Trustworthy Digital Repositories. For example, criterion C34 requires staff at organizations to protect the integrity of repositories and their contents [4, 11]. In particular, criterion C34 requires staff at organizations to protect the integrity of repositories and their content. To accomplish this, the security documentation for TDRs includes specific criteria pertaining to security as part of recent standards for Trustworthy Digital Repositories.
of residual risk is acceptable. Furthermore, they ask staff about their plans to test and further develop their digital repository staff members should identify their objectives. Second, digital repository staff members should self-audit their repositories to ensure security or their perceptions of the said security criteria. Third, digital repository staff members should incorporate confidentiality, integrity, and availability at their digital repositories. Although alternative models of security exist, all seem to address confidentiality, accountability, the security guard that generates the requirement for actions of an entity to be traced uniquely to that entity, in defining trustworthiness [17, p. A-1]. As another example, OECD guidelines proposed nine security principles: awareness, responsibility, response, ethics, democracy, risk assessment, security design, implementation, and reassessment [12]. Stoneburner, Hayden, and Feringa [17] proposed thirty-three principles related to having a security foundation, risk, ease of use, effectiveness, reducing vulnerabilities, and designing with the network in mind. Parker [13] extended the classic Confidentiality-Integrity-Availability (CIA) triad by adding three dimensions: possession, confidentiality, and utility. After a thorough review of the literature, Cherdantseva and Hilton [3] proposed extending the CIA triad to an Information Assurance and Security (IAS) octet consisting of: confidentiality, accountability, auditability, authenticity/trustworthiness, non-repudiation, and privacy. It is important to note that Cherdantseva and Hilton had IAS academics and experts evaluate the IAS octet. According to Cherdantseva and Hilton, the IAS octet is part of a larger, all-encompassing reference model of information assurance and security. Although alternative models of security exist, all seem to incorporate confidentiality, integrity, and availability at their core.

In addition to multiple definitions of security, the literature on security in computer science also offers some security metrics. For example, Bower and Sugumaran [2] provide assessment metrics such as properties, measurement of adherence to secure coding standards, monitoring and reporting of security status, and gauge the effectiveness of various security controls [10]. Although some security metrics exist, researchers acknowledge that security is actually quite difficult to measure. Pfeifer and Cunningham [14] list nine reasons why security is hard to measure:

- We can’t test all security requirements,
- Environment, abstraction, and context affect security,
- Measurement and security interact,
- No system stands alone,
- Security is multidimensional, emergent and irreducible,
- The adversary changes the environment,
- Measurement is both an expectation and an organizational objective,
- We’re overoptimistic, and
- We perceive gain differently from loss.

While some components of the threat modeling process are qualitative, quantifying the risk of threats enables system administrators to rank the order in which threats should be addressed. Within the computer science literature, various approaches have been proposed for characterizing and quantifying the threat of threats, including calculating risk as the product of the damage potential and the likelihood of occurrence, Risk = Criticality × Likelihood of Occurrence [8].

Both DIN 31644 and ISO 16363’s security requirements draw upon an earlier standard for TDQs: Digital Repository Audit Method Based on Risk Assessment known as DRAMBORA [5]. For this study, we recommend that digital repository staff members use DRAMBORA as a tool for performing risk assessments. Similarly, DIN 31644 recommends that digital repository staff members use DRAMBORA to help identify the sections of the archive which are worth preserving, analyze any potential threats to the specific archive, and perform risk assessments of possible damage scenarios.

The DRAMBORA methodology consists of six steps. First, digital repository staff members identify objectives. DRAMBORA includes a list of examples of objectives for digital repository staff members to choose from. Second, digital repository staff members identify activities that are necessary to achieve their objectives and assets, including human resources and technological solutions, that are central to achieving security objectives. Third, digital repository staff members should align risks to their activities and assets. This step requires digital repository staff members to document the specific risks associated with each activity and asset. Here a single risk may associate with multiple activities, or vice versa. Fourth, digital repository staff members should assess, avoid, and treat risks by characterizing each risk’s “probability, impact, owner, and the mechanisms or proposed mechanisms by which it can be avoided or treated” [5, p. 39]. Fifth, digital repository staff members should complete a risk register listing all identified risks and the results of their analysis and evaluation. Also known as a risk log, it should include information about the status of each risk and include details that can help digital repository staff members in tracking and monitoring risks.

Taken together, standards for TDQs underscore the importance of security and provide relatively similar recommendations to digital repository staff members about how to address security. However, the security criteria themselves do nothing to illuminate actual digital repository staff members’ perceptions on security or their perceptions of the said security criteria.

2.2 Security in the Computer Science Literature

Relevant to a discussion on security in the digital preservation literature is discussion of security in the computer science literature. In digital preservation, the primary focus is on the security of digital repositories and their content. On the other hand, in the field of computer science security is more encompassing, including a broad range of computing infrastructures, not just digital repositories. Computer science also has a longer, more established body of literature on security, including definitions and metrics for the concept.

Computer scientists who specialize in security research have reached a consensus that computer security consists of at least three main principles: confidentiality, integrity, and availability. Confidentiality refers to concealment of information or resources, integrity refers to the trustworthiness of data or resources, and availability refers to the ability to use the information or resource desired [1]. While security researchers seem to agree on these three principles of security, others have proposed additional security elements. For example, some researchers have recommended including the concept of accountability, “the security guard that generates the requirement for actions of an entity to be traced uniquely to that entity, in defining trustworthiness [17, p. A-1].” As another example, OECD guidelines proposed nine security principles: awareness, responsibility, response, ethics, democracy, risk assessment, security design, implementation, and reassessment [12]. Stoneburner, Hayden, and Feringa [17] proposed thirty-three principles related to having a security foundation, risk, ease of use, effectiveness, reducing vulnerabilities, and designing with the network in mind. Parker [13] extended the classic Confidentiality-Integrity-Availability (CIA) triad by adding three dimensions: possession, confidentiality, and utility. After a thorough review of the literature, Cherdantseva and Hilton [3] proposed extending the CIA triad to an Information Assurance and Security (IAS) octet consisting of: confidentiality, accountability, auditability, authenticity/trustworthiness, non-repudiation, and privacy. It is important to note that Cherdantseva and Hilton had IAS academics and experts evaluate the IAS octet. According to Cherdantseva and Hilton, the IAS octet is part of a larger, all-encompassing reference model of information assurance and security. Although alternative models of security exist, all seem to incorporate confidentiality, integrity, and availability at their core.

While quantifying risks will enable us to capture an organization’s perception of risk. Pfeifer [15] advises that we should avoid false precision by doing the following:

- Base the probability distribution of a threat/attack occurring on historical data, not just on expert judgment;
- Since both scientists and lay people may understand the concept of probability and useability in small samples of data, particularly when the results are consistent with preconceived, emotion-based beliefs", we are to be mindful of the size of our experiments and the scalability of our results.

While measuring security is difficult, and few security metrics of any kind exist, metrics for understanding perceptions of security are particularly scant.

Taken together, the literature on security in digital preservation and computer science stress the importance of security, while also leaving several open research questions. This study focuses on four of them:

1. How do digital repository staff members think about the security of Trustworthy Digital Repositories?
2. What are digital repository staff members’ attitudes toward security criteria in standards for Trustworthy Digital Repositories?
3. How relevant are security principles that have been established in the computer science domain to digital repository staff members’ concept of security?
4. Is it possible to develop a survey that could serve as a tool for measuring digital repository staff members’ perceptions of security for Trustworthy Digital Repositories?

3. METHODS

To address the research questions, we conducted interviews with digital repository staff members at organizations whose repositories have attained formal, third-party trustworth status. We also administered surveys to those individuals. The purpose of using these data collection methods was to understand how the participants thought about security and to assess measurement of the concept. While various standards for trustworthiness of digital repositories exist [4, 6, 9], at present, DIN 31644 is the only standard that:

1. has been formally recognized by a standards-granting body, and
2. has organizations whose repositories have been formally certified by third parties. Thus, we decided to include in our study only digital repository staff members whose repositories have recently acquired nestor seals of approval. During April 2016, we recruited and successfully acquired nestor seals of approval. During April 2016, we recruited and successfully acquired nestor seals of approval. During April 2016, we recruited and successfully acquired nestor seals of approval.

3.1 Interviews

During semi-structured interviews, participants discussed their definitions of security and trustworthiness. They also discussed their views on the relationship between the trustworthiness of digital repositories and their security. Afterwards, participants discussed security criteria in DIN 31644 (e.g., criterion C34), including how much difficult they thought it was to address the criteria, how they reported to test the criteria, how they addressed the criteria, whether they thought the criteria were sufficient, and what, if any, additional changes they would recommend. Participants also discussed the extent to which they thought their repositories were more secure as a result of adhering to these criteria. Appendix A includes the
All interviews were audio-recorded and transcribed. Participants reported working approximately five to nine years as policy and services development within their organizations. Two people participated in this study, one from each organization where they worked. Their responsibilities included overseeing teams involved in national and international digital preservation projects and initiatives as well as policy and standards development within their organizations. Participants reported working approximately five to nine years on digital repositories at their current organizations. Both participants reported having involvement in the development of standards for digital repositories.

### 4.2 Interview Findings

Participants shared their views on the concept of security for digital repositories. Specifically, they viewed security as a prerequisite for trustworthyworthiness. They saw security as making sure that repositories act as they are supposed to with no intended or unintended interruptions.

Participants also shared their views on criterion C34 and its importance. They thought that criterion C34 is important in general, but the explanatory notes for C34 were a helpful complement, providing guidance on how to successfully address the criterion within their repositories. Despite the fact that participants found it difficult to address criterion C34, they felt prepared to address it based on the security measures they have in place to mitigate any threats. They wanted to understand what impact digital repository staff members’ views might have on the success of their security efforts. We felt these individuals would be in the best position to evaluate the security standard would be in the best position to evaluate the security criteria without insight into the perspectives of those who are responsible for actually addressing those criteria. Specifically, two members of the research team coded the interview notes for criterion C34 set the bar for security too high, too low, or just right, participants stated that addressing the explanatory notes sets the bar just right, suggesting that they considered the security requirements for repository certification as reasonable, appropriate, and sufficient for securing their repositories.

Analysis of interview data against the concept of security, integrity, and availability security principles established in computer science literature revealed that participants provided statements pertaining to the concept of integrity most frequently, followed by availability and confidentiality. Table 1 lists the frequency with which participants provided statements pertaining to each concept. When participants mentioned integrity, they referred to protecting their data from any threats, including manipulation. Participants mentioned the importance of integrity and availability because both are included in the nested definition of security—a definition which they reported as being important to their work. They did not feel completely confident on what either of the concepts meant to them in their practice.

### 4.3 Survey Findings

To complement the interview data and get a better sense of the relevance of security principles to the participants, we administered surveys to them. The surveys asked questions about participants’ views on aspects of confidentiality, integrity, and availability.

Table 2 lists the mean scores of participants’ responses to the surveys questions pertaining to each security principle. Comparing the mean scores of participants’ responses reveals that participants are most concerned with integrity, followed by availability and confidentiality.

<table>
<thead>
<tr>
<th>Security Concepts</th>
<th>Frequency</th>
<th>Mean Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>2</td>
<td>3.88</td>
</tr>
<tr>
<td>Integrity</td>
<td>10</td>
<td>4.55</td>
</tr>
<tr>
<td>Availability</td>
<td>2</td>
<td>3.75</td>
</tr>
</tbody>
</table>

A Kruskal-Wallis H test showed that there was a statistically significant difference in participants’ ratings of security survey items based on the different principles the items referred to, \(H(2) = 7.82, \ p = .02\), with a mean rank security score of 13.75 for confidentiality, 23.50 for integrity, and 14.25 for availability. These results suggest that participants had stronger attitudes relative to their attitudes about availability and confidentiality.

### 5. DISCUSSION

Results underscore the importance of the security to digital repository staff members who participated in this study. Participants mentioned the three security principles of confidentiality, integrity, and availability during the interviews. Participants also rated survey items pertaining to those three principles higher suggesting that they are relevant to their views on securing digital repositories.

Although participants mentioned the three security principles of confidentiality, integrity, and availability during the interviews and rated survey items pertaining to them highly, results of this study are empirical evidence for some principles of security than others. For example, participants provided more statements related to integrity than availability and confidentiality. As another example, participants rated survey items pertaining to integrity higher than survey items pertaining to availability and confidentiality. The fact that the interview data and survey data triangulate with respect to more emphasis on integrity relative to availability and confidentiality is interesting and needs to be looked at more in depth in future research.

To understand whether having more questions pertaining to the concept of integrity has an effect on the results. Second, we need to understand whether we would still receive more empirical support for integrity than availability or confidentiality if a similar study was conducted with a larger sample. This would enable us to know if the study participants’ views on security generalize to other digital repository staff members. Third, we need to understand whether having more security criteria without insight into the perspectives of those who are responsible for actually addressing those criteria. Specifically, two members of the research team coded the interview notes for criterion C34 set the bar for security too high, too low, or just right, participants stated that addressing the explanatory notes sets the bar just right, suggesting that they considered the security requirements for repository certification as reasonable, appropriate, and sufficient for securing their repositories.

Analysis of interview data against the concept of security, integrity, and availability security principles established in computer science literature revealed that participants provided statements pertaining to the concept of integrity most frequently, followed by availability and confidentiality. Table 1 lists the frequency with which participants provided statements pertaining to each concept. When participants mentioned integrity, they referred to protecting their data from any threats, including manipulation. Participants mentioned the importance of integrity and availability because both are included in the nested definition of security—a definition which they reported as being important to their work. They did not feel completely confident on what either of the concepts meant to them in their practice.

### 4.4 Findings

The findings are based on the methods we used to collect the data. After discussing participant characteristics, we discuss findings from the interviews. We next discuss findings from the surveys.

<table>
<thead>
<tr>
<th>Security Concepts</th>
<th>Frequency</th>
<th>Mean Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>2</td>
<td>3.88</td>
</tr>
<tr>
<td>Integrity</td>
<td>10</td>
<td>4.55</td>
</tr>
<tr>
<td>Availability</td>
<td>2</td>
<td>3.75</td>
</tr>
</tbody>
</table>

The primary limitation of this study is its sample size. Only two digital repository staff members participated in this study. Thus, we cannot generalize the results of this study beyond our sample. However, we felt that who participated in this study was more important than how many. We needed individuals who were at organizations where third parties had verified the success of their security efforts. We felt these individuals would be in a better position to evaluate the security criteria within the standard. These issues guided our choices regarding who was eligible to participate in our study, which in turn, led to a small sample size. Despite our small sample size, we reached 100% of our sampling frame; representatives from all of the organizations who provided approval participated in this study. It is also important to note the challenges to employing traditional research methods, such as interviews and surveys, to study security. For example, people are reluctant to participate in security studies because: 1) they have concerns about whether the information they provide will be used inappropriately, such as in marketing, or 2) they fear their own shortcomings with respect to their expertise might become exposed as a result of participation [18]. Although we faced a number of these well-documented

![Security Concepts](security_concepts.png)
challenges to recruiting participants for our study, we were yet able to successfully recruit individuals from both organizations that recently acquired nestor seals of approval.

6. CONCLUSION
Security is a major issue for digital repositories. Digital repository staff members are responsible for managing and securing digital repositories, thus their perspectives on security are critically important to understand. This study provided a preliminary investigation into digital repository staff members’ views on security and security criteria in standards for TDRFs, in particular DIN 31644 and the nestor explanatory notes for Trustworthy Digital Archives. Participants articulated their views on security in terms of integrity and to a lesser extent availability and confidentiality. Results of this study warrant a closer correspondence between research on security in digital preservation and computer science, because of the overlap that results of this study have demonstrated. Participants in this study found the security criteria in the standard that they chose sufficient. Going forward, researchers should continue analyzing digital repository staff members’ views on security and security criteria, so that the digital preservation community can validate the relevance and importance of the security criteria by those who are responsible for making digital repositories secure.

7. ACKNOWLEDGMENTS
We thank Michael Frisby and his colleagues at the Indiana Statistical Consulting Center for providing assistance with data analysis and reading prior drafts of this work.

8. APPENDICES
8.1 Appendix A – Interview Protocol
1. How do you define repository trustworthiness? In other words, what does it mean to you for a repository to be trustworthy?
2. How do you define security as it relates to digital repositories? In other words, what does security mean to you?
3. How would you describe the relationship between the trustworthiness of a digital repository and the security of that digital repository? In other words, how would you describe the relationship between security and trustworthiness?
4. Take a minute to read over C34, the nestor criterion on security. Now think back to when you were preparing for audit. How easy or difficult was it to address criterion C34?
5. How much time do you think it took you and your colleagues to address criterion C34?
6. How prepared were you and your colleagues to address criterion C34?
7. Do you think your repository is more secure as a result of addressing criterion C34? Why or why not?
8. Do you think criterion C34 sets the bar too high for addressing security issues? Or do you think criterion C34 sets the bar too low for addressing security issues? Or do you think criterion C34 sets the bar “just right” for addressing security issues? Why or why not?
9. Do you think any additional criteria should be added to criterion C34 to make digital repositories more secure and therefore more trustworthy? If so, how would you describe what criteria should be added?
10. Did you use DRAMBORA to help you address the security criteria in DIN 31644? If so, which parts of DRAMBORA were most helpful and why?
11. Is there anything else you’d like to add, given our topic of security of Trustworthy Digital Repositories?

8.2 Appendix B – Security Perceptions Survey
Questions pertaining to confidentiality (Questions were answered on a 5-point, likert-type scale ranging from “Strongly disagree” to “Strongly agree” with one additional option: “Not applicable.”)
1. Access control mechanisms should be used to support confidentiality (e.g., cryptography).
2. Mechanisms should be used to prevent illicit access to information.
3. The existence of data should be denied to protect it.
4. Resources should be hidden to protect them.

Questions pertaining to integrity (Questions were answered on a 5-point, likert-type scale ranging from “Strongly disagree” to “Strongly agree” with one additional option: “Not applicable.”)
1. Improper changes to data should be prevented.
2. Unauthorized changes to data should be prevented.
3. Information about the source of data should be protected.
4. Unauthorized changes to information about the source of data should be prevented.
5. Prevention mechanisms should be used to maintain the integrity of data by blocking any unauthorized attempts to change the data.
6. Prevention mechanisms should be used to maintain the integrity of data by blocking any attempts to change the data in unauthorized ways.
7. Detection mechanisms should be used to report when the data’s integrity is no longer trustworthy.
8. System events (e.g., user or system actions) should be analyzed to detect problems.
9. The data itself should be analyzed to see if it has been changed.
10. A system should report when a file is corrupt.
11. A system should report that when a file is corrupt.

A system should guard against denial of data attacks.
A system should guard against denial of service attacks.
An unavailable system is at least as bad as no system at all.

4. A system administrator should be able to tell the difference between when data is not available due to circumstances in the environment versus a security attack.

9. REFERENCES