Sysadmins and the Need for Verification Information

Nicole F. Velasquez  
The University of Arizona  
1130 E Helen St  
Tucson AZ 85721-0108  
nicolefv@u.arizona.edu

Alexandra Durcikova  
alex@eller.arizona.edu

ABSTRACT
Traditional usability measures may not be sufficient for some specialized users, such as system administrators. Because of their broad range of responsibilities for highly complex and risky business environments, these users also need tools that are powerful, informative, and credible. To do their work, system administrators need the ability to verify the work they have done. That verification comes from accurate and available information that we refer to as information credibility. This exploratory research aims to address the relationship between task complexity, task risk, and verification information seeking in GUI tools used by system administrators. Potential antecedents of information verification are identified and a model is proposed that addresses how aspects of the task and environment affect the need for verification. Findings suggest that task complexity is a significant indicator of the need for verification information. Armed with this knowledge, practitioners can anticipate the needs of system administrators and design GUI tools with information credibility in mind.

Categories and Subject Descriptors
H.5.2 [User Interfaces]: Screen design, graphical user interfaces. K.6.4 [Systems Management]

General Terms
Design, Human Factors, Verification

Keywords
System administrator, information seeking, verification, usability

1. INTRODUCTION
When designing software applications, the design team often considers usability, ease-of-use, and aesthetics [1-3]. But for some end users, these well-known and well-tested design principles may not be sufficient. With responsibilities that include the installation, configuration, monitoring, troubleshooting, and maintenance of increasingly complex and mission-critical systems, system administrators (sysadmins) require usable interfaces and applications that are also powerful, informative, and credible [4, 5]. Although many vendors offer GUI tools for administrators, sysadmins often augment those tools with homegrown, verified CLI scripts and spreadsheets [6].

With the health of a network and its systems dependent upon one or a few people and their tools, are standard GUI usability design principles adequate for system administrators? Sysadmins represent a unique user group in that they are considered technical experts and are often solely responsible for large-scale, complex, high-risk environments that require constant understanding of both general (e.g., current system state) and specific (e.g., the names and locations of data backup servers) network information. Historically, system administrators have relied on direct communication with the servers and network they are responsible for by using cryptic – but powerful and informative – command line interfaces. While the graphical user interfaces designed and deployed today are more usable, do they provide the end user with enough power and information to effectively replace the command line?

Today’s business infrastructures are comprised of multiple components (e.g., database management servers, application servers, and web servers) residing on hundreds of servers distributed across many networks and running on multiple operating systems. Disaster recovery and backup systems add complexity to the environment and the requirements for data availability have amplified both the importance of continuously available data and the cost of system downtime. Because this infrastructure must be managed nearly flawlessly, the industry has seen system management costs exceed system component costs [7-9]. Though many companies are exploring automated system management [7, 10, 11], system administrators are still ultimately responsible for the management and coordination of the entire system and often represent the single point of failure. In conclusion, the work of system administrators can be complex and risky.

Even with such an important and critical role, little HCI research has examined the particular needs of system administrators. The importance of usability [3, 12-17], ease-of-use [18, 19], end-user satisfaction [1, 20-23], and task-technology fit [24-29] are well-documented and validated in the literature. Barrett et al. [30] call for a focus on system administrators as unique users within HCI research, citing the unique problems they face because of the complex and risky systems they manage and their power-user authorities and skills.

While an application may be well designed and usable, the complexity of a system administrator’s job and the high-risk environments in which they work necessitate credibility in the increasingly automated tools provided by vendors, especially when errors or failures often result in blame to the system.
A 2003 field study of system administrators illustrates the role of information credibility in an inherently complex and risky situation, system troubleshooting [4]. Throughout the authors' experiences and examples, key components of credibility are reported. These aspects are dependent upon information accuracy and availability, namely integrity, consistency, transparency, communication, and sharing. Other recent work has shown that system credibility plays a major role in system administrator interface choice [5]. In their study, a survey of system administrators was conducted to examine how psychological human-system credibility affects their preferences and eventual use of Graphical User Interfaces (GUIs) or Command-Line Interfaces (CLIs). With a majority of sysadmins using CLIs exclusively (65%) or in conjunction with GUI tools (22%), two findings of this study highlight the importance of information accuracy, with survey respondents reporting (1) greater overall CLI information accuracy, and (2) an incorrect or incomplete report of system state by the GUI, which reflects less information availability and accuracy. These studies all show that system administrators need – and are motivated to use – credible systems that provide them with the accurate and available information they need to perform their jobs.

The work of system administrators is, as shown above, complex and risky. To do their work, sysadmins need and will use credible systems that give them the ability to verify the work they have done. That verification is made possible by accurate and available information, or information credibility. This research focuses on system administrators’ work, their need for verification information, and therefore their need for credible systems. By keeping the need for accurate and available information in mind, practitioners can address these issues in the design of their user interfaces.

2. BACKGROUND

Data management has evolved over the years from one of manual hard copy tracking to today’s complex and intricate data management systems that capture and store richer data types [31]. With the automation of more and more systems and greater importance being placed on capturing all relevant data, data management systems must be powerful, flexible, and fault-tolerant. Further complicating the situation is globalization and the need for continuously available data. Even overnight system outages for data backup are often not tolerated [32]. Today’s data management systems are comprised of dozens of networked hardware and software components strategically combined to better and more easily manage complexity and lower the total cost of ownership [33]. Recent hardware advances have shifted the primary cost of data management from hardware and software to the human component needed to set up and oversee the infrastructure, doubling the relative system administration cost in the last ten years [34, 35]. The high cost of system administration emphasizes the need for tools suited to this unique user group.

Despite a population of about 2 million [36], system administrators are not well represented in HCI literature, though recent research has begun to focus on this important user group. A CHI 2003 conference workshop called attention to the timeliness and importance of designing for system administrators [30]. This workshop addressed the benefits associated with tool design specific to system administrators, such as decreased cost and increased system services and availability, while emphasizing the unusual problems faced because of the complex and high-risk tasks and environments the system administrators must work with. One important issue identified in the workshop was system monitoring and notification, with a credible system providing accurate system state information essential to the task. Researchers conducted an exploratory study of system administrator situation awareness through preliminary interviews and a short survey broadcast via Internet newsgroups [37]. The study’s 54 non-random respondents limit its generalizability, but one interesting finding was the relative incompleteness of the system administrators’ mental models. They reported uncertainty of 23% of their expertise domain, suggesting a need for credible tools that can provide information about the system, its state, and its processes. Barrett et al. [6] conducted field studies in large corporate data centers and reported on system administrator tool use in environments they identified as ones of "significant risk, system complexity, and system scale" (p389). One finding of this research was the amount of time spent diverted from their tasks because of missing system information. In guiding successful tool development for system administrators, they point out fundamental issues such as truthful information, immediately available feedback, and presentation of information.

There seem to be two aspects of credible systems in terms of the information they provide: availability and accuracy. Intuitively, information availability can manifest itself as simply the reporting of information by the system. As seen above in the studies by Hrebec and Stibler [37] and Barrett et al. (2004), system state information availability may not only lie in the actual availability of the data, but also in the timely availability of data, e.g., the report of current system state. Additionally, not only must the information be available, but also it must be accurate. Information accuracy can manifest itself as an accurate report of system state or the progress of system processes. Information accuracy can also be reflected in the quality and completeness of information presented, as found in a study investigating error messages [38]. This research found that the content of error, warning, status, and other messages played a fundamental role in how system administrators think and react to the situation at hand. Not only did the information convey a message, but accurate information guided the user’s problem-solving behavior. Furthermore, inaccurate or incomplete information led to frustrations and a decrease in credibility granted to future messages.

3. THEORETICAL FRAMEWORK AND MODEL DEVELOPMENT

Recent work defining computer credibility proposes that credibility matters when a computer system: acts as a knowledge source, instructs or tutors users, acts as a decision aid, reports measurements, runs simulations, renders virtual environments, reports on work performed, or reports on its own state [39, 40].
With most system administration tools performing at least one if not many of those functions, system credibility is clearly important to system administrators and worthy of research. Following the suggestion of Fogg and Tseng [39] that the aspects of system credibility can be studied individually, this research focuses on information credibility, or the believability of system-supplied information. The other three aspects of system credibility are device credibility, which is reflected in the physical dimensions and design of the computing product; interface credibility, or the physical display and interaction with the system; and functional credibility, which is seen in what the system does and how it is done. Two dimensions of system credibility are also identified; this research will focus on the system expertise dimension, which is concerned with the underlying knowledge and skill of the system, as reflected in information availability and accuracy; as opposed to trustworthiness, which addresses the perceived goodness and morality of the system.

Fogg and Tseng [39] suggest that varying levels of risk and complexity are potential independent variables, but no relationship has been tested yet. Kandogan and Maglio [4] indicate that additional information and verification (through transparency and communication) may increase a system’s information credibility; a better understanding of situations that lead a user to seek that verifying information would allow practitioners to anticipate those needs and include that information in their systems. Little has been done, however, to identify the antecedents of this particular information seeking behavior. This research aims to address the relationship between task complexity, task risk, and verification information seeking in GUI tools used by system administrators. Potential antecedents of information verification are identified and a model is proposed that addresses how aspects of the task and environment affect the need for verification.

The model proposes that greater task complexity will increase the need for another type of information, verification information, and that greater task complexity will increase the amount of verification information sought. The model also proposes that the greater risk associated with the task will increase the need for information verification. These relationships are shown below in Figure 1.

To investigate the research model identified above, two hypotheses are tested. Each hypothesis relates to the antecedents of verification information seeking behavior used to reassure the user and increase the information credibility of the GUI tool being used.

Traditionally, task completion is defined as the actual execution of the task [41]. Studies about task completion and information seeking behavior, then, cease to record user behaviors after actual task execution but potentially before the user has moved on to another task. Based on our observations with system administrators, we propose that a task has two components: actual task execution and task verification (see Figure 2), each of which has its own associated information types.

**Figure 2: Components of task completion and associated information types.**

<table>
<thead>
<tr>
<th>Task Completion</th>
<th>Task Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Components</td>
<td>Information Types</td>
</tr>
<tr>
<td>Task Execution</td>
<td>Problem Info</td>
</tr>
<tr>
<td>Task Verification</td>
<td>Problem Solving Info</td>
</tr>
<tr>
<td>Domain Info</td>
<td>Verification Info</td>
</tr>
</tbody>
</table>

Work done by Bystrom and Jarvelin [42] investigated the role of task complexity in information seeking behaviors. They based their work on the information seeking model proposed by and Mick [43] that suggests that environmental and situational constraints, including task complexity, play a major part in determining information seeking behavior. Bystrom and Jarvelin used questionnaires and diaries to collect data about how higher civil servants completed job tasks. They identified five levels of task complexity and investigated the number and types of information sought in the execution of those tasks. Their research identified three types of information sought during task execution: problem information, which is the structure, properties, and requirements of the problem at hand; problem solving information, which are the methods of problem treatment; and domain information, which is the known concepts, laws, and theories in the problem domain. Their findings suggest that as tasks increase in complexity, both the amount and types of information sought in task execution also increase. The identification of the second component of task completion above, task verification, leads to the identification of another type of information that we will call verification information. Verification information is the echoed or repeated outcome of the task or subtask that has already been executed. Following the findings of Bystrom and Jarvelin [42], this research theorizes that as task complexity increases, both the number and types of information sought will also increase, which will be reflected in (a) the user seeking another type of information, verification information, and (b) the amount of verification information sought. Thus, the following hypotheses are proposed:

**Figure 1: Proposed research model**
H1a: Tasks with greater complexity will lead users to seek another type of information, verification information.

H1b: Higher complexity tasks will lead users to seek more verification information.

While system administrators work in high-risk environments, certain aspects of their job constitute greater risk than others. For example, an error in server installation, though possibly costly, can be discovered and repaired with minimal impact to existing systems and data. This would represent a low-risk task. However, an error in identifying and starting data backup processes may result in lost data and system downtime; this would represent a high-risk task. Marketing research suggests that consumers use the search for additional information as a risk-reducing strategy [44]. Murray studied pre-purchase behaviors of consumers contemplating the purchase of services, which has been identified as being particularly risky [45]. Subjects were presented with hypothetical purchase scenarios, each with varying levels of inherent risk. After reading the scenarios twice, they were given a questionnaire that measured the types, if any, of information sources that would be consulted prior to purchasing the goods presented. Murray found that extended information acquisition is utilized in the purchase of (particularly risky) services and less, if any, information acquisition is utilized in the purchase of (less risky) goods. Accordingly, this paper theorizes that the greater the risk associated with the task at hand, the resulting increase in need for additional information as a risk-reducing strategy. Therefore, the following hypothesis is proposed:

H2: Tasks with greater associated risk will result in a greater need for information verification.

These hypotheses propose that task complexity and task risk are antecedents to a user seeking verification information, which is the information availability and accuracy aspect of information credibility. These links are hypothesized to be positive, with no links proposed to be negative.

4. METHODOLOGY

4.1 Overview

To test the proposed model, audio and video data from a usability study was analyzed. The study focused on a single system administrator tool (pre-beta code release) used to setup, configure, and monitor various data replication tasks. This web-based GUI tool was designed and created by a Fortune 500 company specializing in data management software with system administrator usability in mind. The Fortune 500 company conducted the usability study to assess the tool’s design and spanned four days, observing one system administrator each off the four days. The participants were seated in a conference room physically separated from the servers and systems they were controlling.

Each participant was carefully selected and interviewed by a screener to ensure an adequate level of responsibility and expertise. Of the four participants selected, two were familiar with the data management company’s software products and used them in their day-to-day activities, while the other two participants used products from a competitor. All four participants indicated high-levels of system administrator experience and all were currently responsible for their company’s data management and replication. Each participant received a $300 honorarium as compensation, in addition to reimbursement of all travel expenses.

At the beginning of each one-on-one session, an open-ended interview was conducted, which usually lasted 15-20 minutes. This discussion gathered information on the user’s primary and secondary responsibilities, what their morning routine consisted of, and what reporting or metrics management requested from them. They were also given the opportunity to describe a good day, a bad day, and an ideal process for maintaining the availability of mission critical data in the event of a primary site failure. Following this interview, the participants were given 20 tasks one at a time. Each task covered some aspect of data management or replication and users were encouraged to think aloud and share any comments or observations. As was stated earlier, credible information needs to be both available and accurate. Because we were primarily interested in the availability aspect of information credibility, participants were assured that the information presented by the software application was accurate.

4.2 Variables

Three constructs were measured to test the proposed research model: task complexity (TC), associated task risk (TR), and need seeking of verification information (VI). These variables and their operationalizations are discussed below.

While task complexity can be defined as a subjective measure [46] or a relational measure [25], problems with construct validity [47] and generalizability [48, 49] suggest that a theory-based objective measure of task complexity is most appropriate [50]. As outlined by Wood’s [49] definition of the task complexity construct, overall task complexity is comprised of its subcomplexities: component complexity, coordinative complexity, and dynamic complexity. Component complexity is a reflection of the number of distinguishable information cues and acts that are required for successful execution of the task. Coordinative complexity is seen in the number and nature of relationships between information cues and acts that are needed for successful task execution. Finally, dynamic complexity is the changes in the system that affect the components and relationships involved in successful execution of the task. This variable was coded along the three categories of low, medium, and high complexity. Task complexity levels were independently coded by two system administrators with expertise in data replication tasks. These coders were not study participants. The coders were given an explanation of Wood’s task complexity framework and illustrative examples of representative tasks in relation to the framework. Following the discussion, each coder was given a list of the tasks and asked to rate each task on a 3-point complexity scale (e.g., low, medium, or high) based on the task complexity
definitions and framework proposed by Wood. Once the raters were complete, any differences in rated task complexity were discussed and negotiated, resulting in 100% inter-rater reliability.

Risk can be measured along any of its six identified dimensions of risk. Five dimensions of risk are identified by Jacoby and Kaplan [51]: financial, performance, physical, social, and psychological. The sixth dimension, time risk, was identified by Roselius [52]. The dimensions of risk most relevant to the system administrator tasks in this study are financial, performance, and time. Financial risk involves possible financial loss or consequences; in the case of this study, there is a financial component to any data loss or system downtime. Performance risk can be reflected in a decrease of personal or system performance; specific performance risk concerns in this study include any system performance degradation or system downtime. Finally, time risk includes the potential loss of convenience or time; for system administrators, the time spent finding, troubleshooting, and fixing any resulting problems represents time risk. Task risk levels were independently coded by the same two system administrators because of their expertise in and knowledge of data replication tasks and associated consequences. Again, these coders were not study participants. The coders were reminded of the components of risk identified above that are associated with an incorrect or incomplete execution of their job tasks. Illustrative examples of low, medium, and high risk tasks were also outlined and discussed. Following the discussion, each coder was given a list of the tasks and asked to rate each task on a 3-point associated risk scale (e.g., low, medium, or high) based on the task risk components identified above. Once the raters were complete, any differences in rated task risk were discussed and negotiated, resulting in 100% inter-rater reliability. Although the participants were observed in a controlled field experiment using test servers and dummy data, we expected that their work experiences and background would influence their knowledge of associated risk and therefore still affect their actions in the study.

A prior study on information seeking behavior [42] classified the type of information being sought and counted the number of information sources sought throughout the task execution process. Because this study was only concerned with users seeking verification information, only user behaviors dealing with verification information were counted. Two measures were recorded from audio/video collected during the usability study: one, a count of the verification information sources sought that were provided by the GUI tool being observed (IN), and two, verification information sources sought that were needed but not made available by the GUI tool being observed (OUT). For example, an OUT source of information verification might come from the user verifying task execution by accessing the server log or expressing the need to query the server for verification information because the GUI did not provide sufficient information. Both IN and OUT sources of information verification were counted to accurately reflect the user’s need for verification information regardless of any information constraints introduced by the design of the GUI tool. Only actions taken to verify information beyond those needed for task completion were recorded. For example, a dialog box indicating the successful execution of the task was not included in the count of verification information sources, but any additional information sources accessed or sought by the user to verify task execution were included in the count. Verification information seeking was independently coded by two individuals, the researcher and another individual familiar with the GUI tool and data replication tasks. The second coder was given illustrative examples of a user seeking verification information. Once the coding was complete, any differences in coded information was discussed and negotiated, resulting in 100% inter-rater reliability.

5. RESULTS

Each study participant was given 20 discrete tasks to perform. After removing tasks that were not completed due to participant choice or an error in the software, a total of 64 tasks were completed. The distribution of the tasks and their associated complexity and risks is given below in Table 1. It should be noted that the testing matrix is not balanced; this exploratory study was based on an analysis of a real usability study and this task distribution reflects realistic situations, where risk and complexity often go together.

<table>
<thead>
<tr>
<th>Table 1. Distribution of Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
</tr>
<tr>
<td>Complexity</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>Grand Total</td>
</tr>
</tbody>
</table>

Example tasks for each complexity (C) / associated risk (R) combination are shown in Table 2.

<table>
<thead>
<tr>
<th>Table 2. Example Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>

The task complexity ratings, associated task risk ratings, and verification information seeking indicators were entered into the binary logistic regression presented in Table 3. Findings show that only complexity had a significant association with seeking verification information. This suggests support for our first hypothesis (H1a), that increased complexity will lead system administrators to seek an additional information type, verification information. Furthermore, the relative effect of a unit change in complexity on the expected odds of seeking verification.
information, which is $e^0$, is 7.163. These results also show that Hypothesis 2, that increased risk leads to an increase in verification information seeking, is not supported. This is surprising, since anecdotal evidence from observations suggested otherwise. One participant even refused to complete a high-risk task, commenting that “clicking the ‘Next’ button here is scary,” even after being reminded of the test environment by the researcher.

**Table 3. Regression on Verification Information Seeking**

<table>
<thead>
<tr>
<th></th>
<th>B</th>
<th>Std. Error</th>
<th>Wald</th>
<th>Sig.</th>
<th>Exp(B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>1.969</td>
<td>0.764</td>
<td>6.634</td>
<td>0.01</td>
<td>7.163</td>
</tr>
<tr>
<td>Risk</td>
<td>0.301</td>
<td>0.72</td>
<td>0.175</td>
<td>0.675</td>
<td>1.352</td>
</tr>
<tr>
<td>(Constant)</td>
<td>-2.374</td>
<td>1.009</td>
<td>5.538</td>
<td>0.019</td>
<td>0.093</td>
</tr>
</tbody>
</table>

Cox & Snell $R^2 = .217$

The task complexity ratings, associated task ratings, and the number of times verification information was sought were entered into the linear regression presented in Table 4. The ANOVA table for the regression, shown below in Table 5, indicates that complexity is not a suitable indicator for the amount of verification information sought by the system administrators in this study. These results show that Hypothesis 1b is not supported, that while an increase in task complexity leads to verification information seeking, it does not necessarily lead to an increase in the amount of verifications sought.

**Table 4. Regression on Total Information Verification Sought**

<table>
<thead>
<tr>
<th>Model</th>
<th>Unstandardized Coefficients</th>
<th>Standardized Coefficients</th>
<th>Beta</th>
<th>t</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Constant)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td>381</td>
<td>-0.521</td>
<td></td>
<td></td>
<td>.731</td>
</tr>
<tr>
<td>Risk</td>
<td>340</td>
<td>-0.149</td>
<td></td>
<td></td>
<td>.883</td>
</tr>
<tr>
<td></td>
<td>368</td>
<td>-0.207</td>
<td></td>
<td></td>
<td>1.230</td>
</tr>
</tbody>
</table>

$R^2 = .108$

**Table 5. ANOVA on Total Information Verification Sought**

<table>
<thead>
<tr>
<th>Model</th>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regression</td>
<td>15.548</td>
<td>2</td>
<td>7.774</td>
<td>3.699</td>
<td>.03(a)</td>
</tr>
<tr>
<td>Residual</td>
<td>128.202</td>
<td>61</td>
<td>2.102</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>143.750</td>
<td>63</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Based on the results above, Hypothesis 1a is supported, while Hypotheses 1b and 2 are not. That is, while higher complexity tasks led users to seek verification information (H1a), they did not lead users to seek more verification information (H1b). Task complexity appears to be the driving force behind the system administrators seeking verification information while doing their jobs.

6. DISCUSSION

This exploratory study has focused on the information availability component of information credibility, presenting system administrator information seeking behavior and one antecedent, task complexity. In that endeavor, it has also expanded the definition of task completion to include both task execution and subsequent task verification. The positive relationship between task complexity and the need for verification information, as evidenced by the seeking of verification information, is a strong indicator of the need for information availability, one aspect of information credibility, in tools designed for system administrators. One simple answer to this need could be the inclusion of a system or console log that echoes any commands sent to the server. A console log would provide system administrators with an efficient way to access the verification information they need within the interface, keeping them engaged with the GUI tool and at their terminal instead of logging directly into the servers or systems they are managing for access to command history.

The findings of this study offer evidence that system administrators may behave differently from others, such as the civil servants studied by Bystrom and Jarvelin [42]. The civil servants worked with people, various information sources, and computers. It makes sense that increasing amounts of information of varying accuracy would be sought when executing increasingly complex tasks (refer to H1b). However, system administrators work with computers and systems whose task verification provides unbiased and accurate system state information, regardless of the number of information sources they seek. For example, if the completion of a system cleanup results in 30% hard disk utilization, the system will report 30% hard disk utilization regardless of the interface used to execute the query. The assumed accuracy of system state information negates the need to probe for multiple information sources; sysadmins need only verify system state once before moving on.

While the observation of actual system administrators contributes to generalizability, the relatively small sample size may limit the findings of this study. Although the relationship between task risk and information verification was not supported, that finding may also lie in the system administrators’ understanding that they were operating on test servers with dummy data; future research may find significance in associated task risk. Another shortcoming of the study was its focus on a single aspect of system administration, data replication. While this is an increasingly important responsibility of a system administrator, it may not contain fully representative tasks. Future research should address these limitations.

In sum, the environment in which system administrators work is one that is both complex and risky. The ability for system administrators to verify the work that they have done is essential and is driven by task complexity. The information seeking behavior seen in this study illustrates the system administrator’s need for information credibility through the availability of verification information. Armed with this knowledge,
practitioners can design system administration GUI tools with information credibility in mind.

7. REFERENCES


