Addressing Human Error through Effective Cyber Policy Design

Katherine Amoresano

The University at Albany community has made this article openly available.
Please share how this access benefits you.

Follow this and additional works at: https://scholarsarchive.library.albany.edu/honorscollege_ehc
Part of the Information Security Commons, and the Science and Technology Policy Commons
Addressing Human Error through Effective Cyber Policy Design

An honors thesis presented to the Department of Homeland Security, Cybersecurity, and Emergency Preparedness, University at Albany, State University of New York in partial fulfillment of the requirements for graduation with Honors in Cybersecurity and graduation from The Honors College

Katherine Amoresano

Research Advisor: Benjamin Yankson, Ph.D.

May 2022
Abstract

Human error is a significant contributing factor to the rise in Cybersecurity attacks regardless of increased technical control implemented to safeguard Information systems. Adversaries can circumvent technical safeguards due to human errors which result from inadequate enforceable policies and training on Cybersecurity for the everyday user. Several studies and articles show that the majority of successful attacks are human enabled, proving the need for human-centric cybersecurity research and practices. This exploratory work reviews the human aspect of Cybersecurity by investigating the cybersecurity policies at SUNY Albany and other SUNY institutions. We used a survey of students and faculty members at SUNY Albany to examine the adequacy of current cybersecurity training and information offered. The result from this work shows that improved Cybersecurity awareness, training, and policies are necessary requirements to significantly affect the degree of errors users make therefore minimizing the chances of Cyberattacks. Based on our literature review and study conducted across selected universities within the SUNY system, we provide recommendations that can inform universities and other institutions of the vulnerabilities and how they can improve their cybersecurity policies and practices to minimize human error as a threat to their information systems components necessary to support ongoing operations.

Keywords: Cybersecurity, Human error, Cybersecurity policies, Cybersecurity training, Cybersecurity controls
Acknowledgments

Throughout the writing of this thesis, I have received a great deal of support and assistance. I would first like to thank my supervisor, Dr. Benjamin Yankson, whose expertise was invaluable in formulating the research questions and in every step of the process. Without his assistance and dedicated involvement, this paper would have never been accomplished.

I take this opportunity to express gratitude to all the College of Emergency Preparedness, Homeland Security, and Cybersecurity faculty members for their help and support during my four years at the University at Albany. I also want to thank my parents for their unceasing encouragement and support.
List of Figures

Figure 1. Percentage of student and faculty respondents .................................................. 12
Figure 2. Survey sent to all participants .............................................................................. 13
Figure 3. How long survey participants have been at the University .................................. 14
Figure 4. Did participants receive cybersecurity training during the onboarding process .... 15
Figure 5. Have employees ever received cybersecurity training while employed by SUNY Albany ................................................................................................................................. 16
Figure 6. Have students received cybersecurity training while studying at the University ... 17
Figure 7. Participants' awareness of responsibility to protect University resources .......... 19
# Table of Contents

Abstract ................................................................................................................................. ii  
Acknowledgments .............................................................................................................. iii  
List of Figures .................................................................................................................... iv  

Introduction ......................................................................................................................... 1  
Literature Review ................................................................................................................ 4  
    A. Cybersecurity Training .................................................................................................. 5  
    B. Behaviors and Attitudes .............................................................................................. 6  
    C. Current Recommendations .......................................................................................... 7  
Method ................................................................................................................................. 8  
    A. Introduction .................................................................................................................. 8  
    B. Research Design .......................................................................................................... 8  
    C. Aim and Objectives ..................................................................................................... 9  
    D. Data Collection .......................................................................................................... 9  
Data Analysis ...................................................................................................................... 11  
    A. Survey .......................................................................................................................... 11  
    B. Qualitative Analysis ................................................................................................... 17  
Discussion and Analysis of Study Result ............................................................................ 19  
Recommendations & Conclusion ......................................................................................... 28  

References .......................................................................................................................... 33
Introduction

Human error in Cybersecurity refers to a variety of mistakes made by users rather than the failure of the computer, technology, or machine being used (Merriam-Webster, n.d.). The mistakes that lead to successful cyberattacks are more commonly coming from human errors, compared to problems with the technology itself (Nobles, 2018). Before the 21st century, the use of computers by everyday users for work was not as prominent as it is today. Presently, there is an increasing number of users that use computers for day-to-day activities at work; therefore, providing more opportunities for attackers to exploit untrained users. A primary issue businesses and institutions face today is the lack of widespread knowledge on providing adequate cybersecurity policies, training, and awareness to staff on how to protect information systems. In recent years, human error in computer security has been the primary reason for breaches, as opposed to having problems with the hardware or software. The current security training in the public sector is inadequate for the frequent human errors encountered. This problem will continue if training methods are not reevaluated and could be detrimental to companies and individuals alike. According to a 2014 IBM study, human error played a role in more than 95% of all security breaches” (International Business Machines, 2014). A subsequent study by IBM in 2019 examined the top three root causes (malicious or criminal attack, system glitch, and human error), which shows that human error accounted for 24% of them. The cost from this cause stayed consistent over the five years during the 2014 to 2019 studies. On average, the cost per year of data breaches caused by human error is $3.36 million (International Business Machines, 2019). While the most common root cause for security breaches in 2019 was malicious actors, human error is one of the top three root causes and must be dealt with accordingly. This is not to
say that there are no problems with the technology itself, but that researchers must take a closer look at why users make mistakes and how to best mitigate them.

Specific to Information System protection, human error can occur at any level within the organization that can result in a data breach. This can range from Executive Officers and IT staff to entry-level employees. For example, System Administrators can make mistakes during system configuration, application and management of security patches, and by implementing poor authentication procedures, including the use of default user IDs and passwords. Other non-technical employees can also make mistakes, including the use of weak passwords, sharing of passwords, physically losing devices with protected data on them, staying logged in when leaving accessible computers unattended, accessing unsafe websites and opening unsafe emails, and inadvertent sharing of confidential data by sending it to the wrong email address (Coffey, 2017). Current literature is shifting towards a more human-centric approach to human error in cybersecurity policies. Some works emphasize the need to change the current approach in policies, while others offer recommendations to mitigate successful attacks due to human error. Additionally, "given the number of human-enabled errors in cyber operation proves that technology alone will not eradicate human-induced mistakes" (Nobles, 2018). These findings suggest that there is a dire need to increase the effort in researching the human aspect of Cybersecurity in conjunction with the technological aspect.

Cyber-attacks happen in both the private and public sectors as well as to the millions of people who use a computer or cellphone daily. The attacks can come from many sources such as, "nation-states, criminal syndicates, cybervandals, intruders hired by unscrupulous competitors, and disgruntled insiders" (Winnefeld et al., 2016). Furthermore, the consequences of these attacks have the potential to be catastrophic for the users or organizations involved. Some
examples of mistakes committed by users or network administrators are failures to patch vulnerabilities in legacy systems, misconfigured settings, and violations of standard procedures, which have opened the door to "the overwhelming majority of successful attacks" (Winnefeld et al., 2016).

Currently, the State University of New York (SUNY) allows different institutions under the umbrella of the SUNY system to have different information security policies as compared to an enforced uniformed SUNY system-wide information security policy that is consistent. But the advantage is that a particular SUNY institution can create policies that best fit its needs. However, with 64 independent policies for each school, a disadvantage is that it allows for fluctuating degrees of security and accountability. This has resulted in varying levels of accessibility, security, inconsistency, and comprehensibility of the policies when evaluated across the broad SUNY system. There is a gap in policies that address the varied aspects of human error, for these reasons, this research is directed toward looking at current policies and standard Cybersecurity training methods for SUNY institutions with a primary focus on SUNY Albany and how to improve them so that they better address human error. This research aims to address this gap in training by reviewing current security awareness training methods for SUNY University at Albany and comparing them to the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This work investigates several SUNY institutions' Cybersecurity polices, Cybersecurity training and awareness, and finally based on the study findings propose better training methods necessary to reduce human error which can lead to cyber-attacks. The information will be presented in this order, the literature review, the methodology of this research, followed by the results, the discussion, and finally the conclusion, which will be a summary of the issues and recommendations.
Literature Review

The amount of cyberattacks caused by human error has increased substantially in the past decade. According to IBM's Security Services 2014 Cyber Security Intelligence Index, "human error played a role in more than 95% of all security breaches" in contrast to those caused solely by unanticipated vulnerabilities in system security. This report is based on 1000 clients in 133 countries with billions of events per year. Previously, companies and organizations have dealt with issues regarding Cybersecurity by focusing on improving their policies, technology, and security professionals. Some examples are "hiring security experts, developing complete security policies, incorporating advanced security technologies, and continuously training their security professionals" (Khader et al., 2021). As a result of these measures, networks, Operating Systems, and programs are safer and more protected. However, less investment has been put towards increasing security awareness among clients or users, making them the weakest link. Ergo, organized cybercriminals have changed their attention to human elements by developing advanced hacking techniques that exploit clients' trust and tendency to help others (Khader et al., 2021). Some common ways in which attackers target their victims are through online chat forums, phishing emails, identity theft, ransomware, and social engineering. The significance of the human factor in cybersecurity awareness has become predominant in importance due to the continuously growing and dynamically changing cyberattack methods, types, and tools (Khader et al., 2021). Therefore, to evade cyber-attacks designed to exploit human factors, it is necessary to create cybersecurity awareness programs and policies that make users aware of the vulnerabilities and their responsibilities.

Evans et al. (2016) found that "50% of the worst breaches in the last year were caused by inadvertent human error," which rose from "31% the previous year". The author's work shows
that half of the significant security incidents that are occurring are a result of specific elements, including users and the unintentional mistakes and errors they make (Evans et al., 2016). Furthermore, Evans examined the complexity of human error regarding cybersecurity policies and presented a current gap in training methods and policies surrounding human error, which has led to a rise in cybersecurity attacks.

Regarding company spending, Blackborrow and Christakis’ 2019 report found that organizations are spending more on security but not wisely. To ensure better use of funds, research done by Lahcen et al. (2020) suggests implementing an interdisciplinary framework for cyber defense that combines behavioral Cybersecurity, human factors, and modeling and simulation. Thus, it is worth integrating human factors into security frameworks to improve the working environment, mitigate risks, and make the system's probability of failure lower (Lahcen et al., 2020).

A. Cybersecurity Training

In the article by Nixon and McGuinness, they review the human dimension of Cybersecurity by using a framework as a structure with which to consider the many ways humans can affect the security of a system both positively and negatively. In part, they focus on user training because "most often employees are trained in the how of cybersecurity but not the why. As a result, the context of a security procedure or process is not fully understood" (Nixon & McGuinness, 2013). The authors go on to explain how one consequence of this is that a user is not able to make dependable risk assessments. They argue that it is crucial that employees feel included in the whole security process so that they assume personal responsibility for maintaining security in the organization (Nixon & McGuinness, 2013). At the same time, because cyber-attacks are rarely encountered by individuals, the necessary skills are rarely, if ever, practiced after initial training"
(Nixon & McGuinness, 2013). This requirement will differ, of course, for different staff roles and responsibilities. This is supported by Coffey's report that indicates that 56% of workers who use the Internet on their jobs receive no security training at all (Coffey, 2017). Coffey further emphasizes that organizations that implement strong technological security procedures still regularly pay insufficient attention to human sources of vulnerability. Such a proposal has been made by several others, including Nixon and McGuinness, in their work "Framing the Human Dimension in Cybersecurity." Nixon and McGuinness emphasized the need for a periodic staff assessment as well as training that updates current threat awareness and minimizes the decline of security competencies, "Over time, staff awareness of cyber threats can quickly fade, while the skills for preventing, detecting and responding to attacks can quickly become outdated”.

B. Behaviors and Attitudes

There has also been research done examining the links between behavior and risky cybersecurity behaviors. In Lee Hadlington's work “Human factors in cybersecurity, examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors," he establishes the link between impulsivity and aspects of information security awareness as well as the attempts to explore how individual differences in personality traits can impact a person's adherence to cybersecurity procedures (Hadlington, 2017).

Furthering the need to study the impact of behavior, Evans et al. (2016) research found that there are metrics that can "identify current vulnerabilities faced, confirm what is an acceptable level of exposure, and address findings based on priority" regarding the technical security aspect (Evans et al., 2016). However, there is no equivalent to this mainstream mechanism for assessment and quantification of human behavior; yet some industries are addressing this by developing techniques using qualitative and quantitative methods (Evans et al., 2016). These
articles ultimately bring us to ask the question, "how can we enhance standard cybersecurity training methods for private-sector employees, in addition to supplementing research on the element of human error in cybersecurity?".

Notwithstanding work done by Hadlington (2017) and Evans et al. (2016), other studies have looked at how personality traits and gender can impact online behavior. Halevi et al. (2013) investigated the correlation between the Big Five personality traits and email phishing responses. The work done by Halevi et al. (2013) confirms that certain personality traits may cause higher phishing vulnerability. The authors (Halevi et al., 2013) demonstrate that with further research, these findings will be useful in the future design of defenses for online attacks. Moreover, this work is supported by Holt (2016), who focused on cybercrime through an interdisciplinary lens. Holt’s work vouches for both computer science and social science researchers to use a holistic approach due to the multiple challenges presented by technological misuse and abuse (Holt, 2016).

C. Current Recommendations

In the current literature, recommendations to optimize human performance have already been made. For example, to develop practices that address human error, Nobles recommends seeking the expertise of human factors specialists and behavioral analysts, conducting a risk assessment solely based on human factors, integrating human factor objectives into the information security strategy, and making humans centric to the foundation of information security and cybersecurity practices (Nobles, 2018). Such recommendations place the importance of the human factor at the top of the list, changing the prioritization of the training from the technological aspect to the human one. Nobles argues that although from the information available, there are quality examples of ways to improve training, further research on improving our cybersecurity training
is important so that human errors are no longer prevalent reasons for system or data breaches. Furthermore, Nobles recommends that colleges and universities should offer to teach and develop human factor courses as well as conduct research projects regarding human factors. He stipulates that companies and organizations need to change what they prioritize in their training, but academic institutions as well need to redirect their focus towards the human factor so that human errors can be minimized (Nobles, 2018).

Security awareness must become integrated into academia because it will ensure that graduates are equipped with the skills and awareness to combat cyberattacks. Work done by Khader et al. (2021) provides a conceptual cybersecurity awareness framework that serves as a guide in the implementation of systems to improve the cybersecurity awareness of graduates in any academic institution (Khader et al., 2021). The goals of the framework are to continuously improve the "development, integration, delivery, and assessment of cybersecurity knowledge into the curriculum of a university across different disciplines and majors" Khader et al. (2021). The use of this framework would lead to better awareness among all university graduates and the future workforce in a variety of areas of study Khader et al. (2021).

**Method**

A. Introduction

This section describes the methodology used for this thesis and the research design, including population, data collection, and data analysis. In this research, the methodology had two parts.

B. Research Design

Most of this research stems from a qualitative design, with some additional quantitative data. One part of the research looked at publicly available information about SUNY, SUNY Albany, SUNY Binghamton, and SUNY Canton’s information security policies, while the other part
consisted of a survey sent to SUNY Albany students and faculty members regarding their experience with cybersecurity training and education. The research was done through the survey for UAlbany students and faculty building on a similar study completed at Columbia University titled, *Measuring the Human Factor of Cybersecurity*. Our study focused on user awareness and vulnerable behaviors, effective training for users, and investigating new methods to measure, quantify, and evaluate the security posture of organizations.

C. Aim and Objectives

There were several objectives for the primary part of the research. The first objective is to assess how easy or difficult it is to find the security policies on the SUNY institution's websites. The second goal is to assess how much the policies incorporate and address the various aspects that encompass human error. The third objective is to use survey responses from faculty members and students at SUNY Albany, to analyze and establish if students and faculty are receiving any sort of information security or cybersecurity training and, if so, what it consists of.

D. Data Collection

Searching UAlbany's website for policies about information security and accepted use was more difficult compared to SUNY Binghamton or SUNY Canton. For example, after searching "information security policies" in the search bar on SUNY Canton's main website, the first link is for their computer and network use policy. It has clear and accessible expectations of its system's users. SUNY Binghamton's ITS policies were relatively easier to find compared to Albany's. When searching for Binghamton's ITS policies, I used Google and Binghamton's website. The searches consisted of the terms and phrases "Binghamton university," "cybersecurity policy,” and “SUNY Binghamton Information Security Policy” on google. On SUNY Binghamton’s website, the searches were more concise. The terms and phrases they consisted of were “IT,”
“information security policy,” and “computer access”. The sequence of pages to find the information security policies on the University website is as such; search “ITS” on the Binghamton university homepage, go to “quick find”, then “about ITS”, then “policies”. On Google, this search method resulted in finding the policies; search “Binghamton university cybersecurity policy” on google and choose the second result.

SUNY Canton only has one policy related to computer and information safety, titled the “Computer and Network Use” policy. Searching for SUNY Canton’s ITS policies was relatively easy when using Google compared to when on the University’s homepage. Using Google to search “SUNY Canton ITS policies” the first result was the Computer and Network Use Policy. From the homepage, searching “its policies” and “policies” did not result in the Computer and Network Use Policy being the first result. When searching “ITS policy,” the Computer and Network Use Policy was the ninth result, and when searching “policies”, a link to the “Policies and Procedures” page was the fifth result. From the Policies and Procedures page, it is possible to get to the ITS policy by clicking on the “Policies and Procedures Manual” which is the first link under the header of the page.

When using the 2021-2022 faculty handbook for SUNY Canton, the Computer and Network Use Policy was found under “Information Services (Computing Policies)”. However, the link for the policy leads to a SUNY Canton page with a 404-error message “the page you are looking for does not exist” (The State University of New York at Canton, n.d.). This is problematic because the information is not accessible, and it could deter users from searching any further due to lack of convenience. Another area of concern is the Computer and Network Use Policy found on the Information Services Policies page says that its last update was 8/17/2009, and it does not include as much information as the Computer and Network Use Policy found on the
Administrative Affairs policy page. SUNY Canton’s website should have the most up-to-date versions of its policies, even if they are on multiple pages.

Utilizing the search bar on the SUNY website, the first search term used was “information security policies”. The results searched within “All of suny.edu”, were not satisfactory because none of them were pages regarding the system’s information security policy. Many results had one of the keywords used in the search but were not the desired result. Using Google to search “SUNY access control policies,” the Information Security Policy was one of the top results listed.

Data Analysis

A. Survey

Overall, the data collected from the survey showed that SUNY Albany students are not aware of their responsibility to protect the University’s resources, nor have they received adequate education or training regarding Cybersecurity or information security. In the survey sent to SUNY Albany students and faculty, there were a total of 25 responses, with 13 of them being from students and 12 from faculty members. As illustrated in Figure 1, 48% of the respondent were faculty members and 52% percent were students. Overall, the response rate was 40%.
As depicted in Figure 2, the survey form presented to the research participants asks about their position and duration at the University, as well as questions regarding their experiences with information security. The second question collected information regarding how long the respondent has been a part of the UAlbany community.
Figure 2. Survey sent to all participants

As per our analysis of the result, in Figure 3, the average number of years respondents have been at UAlbany is 4.5 years, with most respondents being part of the University at Albany community for 3 years. According to the data, some respondents have only been a part of UAlbany for less than a year, while others have been here for 12, 13, or 25 years.
Figures 4 and 5 show the data for questions directed toward faculty members. The question in Figure 4 refers to relates to the onboarding process for faculty. Out of twenty-five respondents, 8% people responded ‘Yes’, 76% responded ‘No’, and 16% responded ‘N/A’. The question in Figure 4 could have been clearer by specifying that it is for faculty since some of the answers under ‘no’ could have been under the ‘N/A’ category. The data shows that not enough faculty members received cybersecurity training when being onboarded. Based on the result, SUNY Albany does not prioritize having its new faculty members made aware of and understand their cybersecurity policies (including information security and accepted use policies).
The next two questions on the survey asked respondents if they have ever received cybersecurity training while employed by UAlbany or while studying at the University. Figure 5 covers the faculty aspect, while Figure 6 covers the student aspect. In Figure 5, 44% responded with ‘Yes’, 36% responded with ‘No’, and 20% responded with ‘N/A’. Figure 6 shows the percentage of respondents who have received cybersecurity training or education while studying at UAlbany. This is targeted at students, but faculty members could also be taking classes at UAlbany. For the question, “Have you ever received Cybersecurity training or education while studying at UAlbany?” 8% responded with ‘Yes’, 56% responded with ‘No’, and 36% responded with ‘N/A’. From this data, one could assume that more faculty than students received cybersecurity training to some degree, however, some students could have answered ‘Yes’ for the question Figure 5 refers to. It is unclear if every faculty member received some training since
there were 12 total responses from faculty members and only 11 respondents who answered ‘Yes’ to if they received cybersecurity training while employed by UAlbany.

**Figure 5.** Have employees ever received cybersecurity training while employed by SUNY Albany
Figure 6. Have students received cybersecurity training while studying at the University

B. Qualitative Analysis

For more information on what the cybersecurity training entailed for UAlbany community members, I asked them to describe it and to be as detailed as they could be. One respondent took the courses CEHC 100 and CEHC 210 during their freshman and sophomore years. These courses are part of the College of Emergency Preparedness, Homeland Security, and Cybersecurity (CEHC). One course, CEHC 100, is the introductory course, and the other, CEHC 210, is the required writing course for the college. CEHC 100 uses lectures, discussion, and case studies for students to develop a broad theoretical, substantive, and practical understanding of the fields of emergency preparedness, homeland security, and Cybersecurity (University at Albany State University of New York, n.d.). CEHC 210 has a focus on critical argumentation, analysis, and communication in the context of emergency preparedness,
homeland security, and Cybersecurity. Students learn to build and evaluate arguments and gather and evaluate evidence by writing briefs and conducting briefings (University at Albany State University of New York, n.d.). While these courses touch on topics relevant to Cybersecurity, the course descriptions do not specifically mention any cybersecurity or information security training.

Many faculty members responded by saying their training consists of a yearly Skillsoft training which includes courses, videos, and compliance sessions, with one of the training sessions being about cyber security practices. The topics that seemed to be covered the most were general cyber hygiene, insider threat, and phishing.

As per one respondent,

As faculty we have a mandated annual online refresher course. It's either mediocre or just plain not very good, and has on occasion contained erroneous or misleading information. I'm skeptical of the impact of user training in general, but I'm very skeptical of the value of this kind of training. Like much of the online mandated training, it feels more focused on box-checking compliance than on attempting to be seriously valuable.

Other respondents had similar views saying that the course provided “rather generic information about phishing, spam, and basic cyber-hygiene practices”, and covered “the different types of attacks (e.g., spear phishing) and the "do's" and "don'ts" of avoiding malware.” Another respondent shared this information about the training,

It was just the skillsoft training, so it was a very basic, unhelpful video lesson about different kinds of cybersecurity threats and basic dos and don'ts (like don't leave your computer open and logged in unattended at a coffee shop). It covered things like phishing and spear-phishing but had little practical guidance in how to spot these kinds of attacks.

These unsatisfactory reviews of the Skillsoft training suggest that Skillsoft needs to review its current Security Awareness for End Users training and that UAlbany should provide end-user training with more accountability and not so “focused on box-checking.” Lastly, the survey touched on how aware community members are of the University’s information security
policies and their responsibilities for protecting university resources. The results, seen in Figure 6, show that most respondents (60%) were not aware of the policies or their responsibilities. It is unclear if the majority of the respondents who answered “No” are students or faculty since the survey did not record this data. This data would be beneficial to have to see if more focus should be put on students, faculty, or both.

![Graph showing awareness of University's Information Security Policies and responsibilities for protecting University resources]

Figure 7. Participants' awareness of responsibility to protect University resources.

Discussion and Analysis of Study Result

Human error is the leading cause of successful cyber-attacks, so this study investigates how the SUNY system and select universities incorporate this aspect in their information security and user access policies. Based on the analysis of the results, SUNY does an appropriate job of setting the standard for its universities’ information security policies. Thus, when evaluated
against the select NIST subcategories, SUNY Albany, Binghamton and Canton do an acceptable job integrating the aspect of human error into their policies.

The SUNY system has a total of five policies in the “Information Security” category, two of which pertain to print resource use. The objectives of the Print Resource Use policy are to “reduce cost, waste, print and paper, simplify and standardize the printer fleet (both single-function and multi-function printers), and secure and optimize the print environment” (The State University of New York, 2021). Since cyber-attacks through printers are not a large concern, this research will not be looking at those policies. Instead, the policies that are examined in this research are SUNY’s Information Security Guidelines and SUNY’s Information Security Policy.

The purpose of SUNY’s Information Security Policy is to help protect SUNY’s information from “unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture” (The State University of New York, 2016). Additionally, this policy aims to clarify the responsibility of SUNY campuses and System Administration regarding existing security policies and procedures. The audience for this policy is “all members of the State University community and users of SUNY data.” People in these groups are expected to adhere to this policy and take the necessary measures to protect and secure the data they possess and transmit (The State University of New York, 2016). The SUNY-wide information security policy states that SUNY institutions must adopt “local campus policies regarding information security,” meaning that there is variation in policies between institutions (The State University of New York, 2016). It is this variation between university policies that this research will be examining.

The results show how universities’ policies fared when compared to selected subcategories in NIST’s Cybersecurity Framework V1.1 Core. This framework is the work resulting from the
Executive Order (EO) 13636 “Improving Critical Infrastructure Cybersecurity”. It is a voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure. The subcategories used to evaluate the policies were chosen based on their relevance to this research and human error. The two categories that the subcategories are in are the Identity Management, Authentication, and Management Control (PR.AC) and Awareness and Training (PR.AT) categories. To examine the policies, they were compared to the informative references of NIST Sp 800-53 Rev. 4 because that is the source that was referenced in NIST’s Cybersecurity Framework V1.1 Core.

The first category in which the subcategories were chosen was “Identity Management, Authentication and Access Control”. The first subcategory selected was, “PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes”, which establishes the necessities for a cybersecurity framework (National Institute of Standards and Technology [NIST], 2015). Additionally, this subcategory is relevant to addressing human error because the policies within it assure that users have the correct privileges and that the authentication method is complex enough (for example, implementing multi-factor authentication). The NIST reference AC-1, one of the informative references, states that an organization’s access control policy should “address purpose, scope, roles, responsibilities, and management commitment” (NIST, 2015). SUNY Albany, Binghamton, and Canton all have access control policies that explain and acknowledge the differences between accounts and who is responsible for them. The SUNY Information Security Guidelines also cover PR.AC-1 by requiring that SUNY Institutions declare campus and policy standards and establish program organization and responsible authorized experts (ISO). Campus and policy standards must communicate “to appropriate members of the campus community the campus
categorization and classification of sensitive information and assets” (The State University of New York, 2008).

For example, SUNY Albany’s Identity and Access Management Policy covers the principles for issuing electronic identifiers (PIN, Albany ID, and Net ID) as well as the authorities responsible for verifying identities, roles, and statuses. Establishing who is responsible for different accounts is beneficial for two reasons. First, it allows for better management because one office or group will not have to keep track of every single account, just the ones they are accountable for. Second, it points users to a centralized location to request help regarding their accounts or other support-related issues. Furthermore, Albany’s Identity and Access Management Policy defines the terms, “electronic identifiers”, “employee”, “student”, “university”, and “university-related organization or organization(s)” (University at Albany State University of New York, 2012). A policy must define its key groups so that users and managers are aware of what group they belong to and what roles and duties pertain to them. SUNY Albany’s Identity and Access Management Policy successfully manages the identities, roles, and responsibilities of its users regarding access to information resources.

SUNY Binghamton also has a University Information Security Program which addresses the departments responsible for information security. As stated in the Information Security Program, the responsible groups are the Information Security Council, University designated staff, Data Stewards, Chief Information Security Officer, IT Security Department, departments or individuals with direct responsibility for tech support, and Data Custodians. The program outlines the organizational and functional responsibilities of these groups as well as their responsibilities concerning information security (such as ensuring proper requirements, controls, and policies are being met) (Binghamton University State University of New York, 2017).
Another aspect of Binghamton’s University Security Program which is ideal is the individual accountability covered by the category of University Data Users. It states, “It is the responsibility of the University data users to protect University information and resources, including passwords, and to report suspected information/computer security incidents as required in the Security Incident Management and Response section of this policy.” (Binghamton University State University of New York, 2017). This policy effectively assigns, manages, and verifies identities and credentials for authorized users, as well as communicates who is responsible for managing certain user accounts and processes.

SUNY Canton’s Computer and Network Use Policy also does a sufficient job of addressing PR.AC-1. Their policy separates identities and roles between students, employees, and public and guest accounts and defines who is included in each account. This is followed by the entities responsible for managing the authorization and termination processes for the various types of accounts. SUNY Canton’s Computer and Network Use Policy also touches on the management’s duties. However, there is not a large difference between responsibilities for different accounts. While the Information Services (IS) Department manages and maintains the operation and integrity of technology systems at SUNY Canton, all users are ultimately responsible for their accounts (The State University of New York at Canton, n.d.).

The following subcategory was PR.AC-2, and deals with physical access to assets. By complying with this subcategory, policies assure that “physical access to assets is managed and protected” (NIST, 2015). Allowing unauthorized users physical access to systems and sensitive information is another way for well-meaning users to unintentionally cause harm to their organization. Therefore, physical access is important to consider when evaluating human error in Cybersecurity and computer use policies. All three universities address physical security;
however, SUNY Albany could go into more depth compared to the other two universities. The SUNY information security guidelines also address physical security by obligating universities to “establish appropriate administrative, technical and physical safeguards to ensure the security of records” (The State University of New York, 2008).

There are two controls from the NIST reference document that these policies were compared against regarding physical access, PE-2 and PE-5. PE-2 states that there should be a list of individuals with authorized access to the facility where the system resides and issuance of authorized credentials for facility access. PE-5 regards physical access to information system output devices to prevent unauthorized individuals from obtaining the output. An output device is any piece of computer hardware equipment that converts information into a humanly perceptible form, such as monitors, printers, copiers, scanners, and audio devices (National Institute of Standards and Technology, 2015).

Regarding physical access, SUNY Albany’s Information Security Policy states that it will include “the administrative, technical and physical safeguards appropriate to the size and complexity of the University and the sensitivity of its information” but does not specify what users should do or what the physical safeguards are (University at Albany State University of New York, 2019). As for the informative references, this policy does not outline the types of individuals allowed access to facilities with sensitive information, nor does it mention how it will safeguard against unauthorized individuals accessing information system output devices.

SUNY Binghamton’s University Information Security Program policy gives more detail about their physical access control mechanisms. Under the section titled “Access Control,” the policy states that the University’s physical control mechanisms are “commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements and ease of recovery
of these assets” (Binghamton University State University of New York, 2017). This policy does a better job of differentiating the levels of security between assets by having corresponding control measures for them. The access control policy goes on to state that it will do this by “ensuring that appropriate information security requirements for user access to automated information are defined for files, databases, and physical devices assigned to their areas of responsibility” (Binghamton University State University of New York, 2017). Additionally, it states which departments are responsible for this.

Furthermore, Binghamton’s Guidelines for Data Security Policy has a section regarding how to control access to rooms and file cabinets where paper records are kept. The three points it touches on are keeping confidential information behind locked doors, prohibiting unescorted guests in areas where sensitive information is in plain sight, and disposing of privileged documents properly in designated recycling or shredding containers (Binghamton University State University of New York, n.d.). While it covers simple aspects of physical access, its inclusion is nonetheless beneficial because of how easy it can be to not obey these guidelines. SUNY Binghamton’s policies regarding access control do an adequate job regarding PE-5 (preventing unauthorized individuals from accessing output devices). As for PE-2, it does not mention having a list of authorized individuals, or even groups, who can access the facility where the system resides.

SUNY Canton partially addresses PE-5 in their Computer and Network Use Policy in various sections. The first section that addresses physical and account security is “Standard Security and Maintenance Practices for All Users.” The maintenance practice it covers is the responsibility of users to “physically secure computers and other devices configured to access the network and logging off systems containing sensitive data before they leave their workspace,
even for a short time” (The State University of New York at Canton, n.d.). This addresses PE-5 by physically restricting the availability and accessibility of information from output devices for unauthorized users. Furthermore, the section titled, “Data Security and Transport of Confidential, Mission Critical, and Personally Identifiable Information” requires that physical security methods must be used at all times, “to protect any removable or easily transported media containing confidential, mission-critical, or personally identifiable information” (The State University of New York at Canton, n.d.). Again, their policy covers accessibility to information from output devices comprising sensitive information. Lastly, the Computer and Network Use Policy prohibits unauthorized access by expecting users to “log off systems, the network, and lock their offices and workspaces when they leave to physically secure client computers.” Most of the responsibility for physical access is placed on the user, which is why everyday users must be made aware of their role regarding information security. Overall, SUNY Canton’s Computer and Network Use Policy sufficiently manages and protects physical access to assets that address NIST’s PR.AC-2 subcategory.

In addition to the subcategory PR.AC-2 dealing with physical access, this work also compares the SUNY University policies against subcategory PR.AC-4 which deals with access permissions, authorizations, and incorporating the principles of least privilege and separation of duties. This subcategory was included because the principle of least privilege, an information security concept where a user is given the minimum levels of access or permissions needed to perform their job functions, is important for mitigating the impact of a comprised account. When setting up and managing accounts, it is crucial to make sure that a user only receives the privileges necessary for their job. If an account becomes compromised, unauthorized access will be limited to only the operations that the specific user has the privilege to perform.
The SUNY Information Security Guidelines address the principle of least privilege when discussing the analysis of practices and protections. It requires that the ISO, or employee of equal stature and responsibility, when analyzing their university’s policies include these two categories: “Access, Identity, Authorization” and “Minimums, Need-To-Know”. The former category includes “practices and protections that limit only to authorized persons and processes the access to ‘Sensitive Information’ and ‘Sensitive Systems’ and limit such access only to authorized transitions and functions”. The latter category encompasses “practices that keep to a minimum, based on business need, the types and instances of ‘Sensitive Information’ used in the business processes and the persons and processes authorized to access it” (The State University of New York, 2008). By ensuring that SUNY universities adhere to these guidelines and categories, the SUNY guidelines comply with the NIST best practice PR.AC-4.

SUNY Albany and SUNY Canton both mention the principles their access management is based on. However, SUNY Binghamton does not mention least privilege in its policies. The NIST informational reference used for subcategory PR.AC-4 is AC-6. This control ensures that the organization implements the principle of least privilege, “allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions” (NIST, 2015). In SUNY Albany’s Identity and Access Management Policy, it states that “access to online services is granted based on the ‘least privilege’ principle” (University at Albany State University of New York, 2021). As shown, SUNY Albany adequately complies with this best practice.

In SUNY Canton’s Computer and Network Use Policy, it declares that all accounts and data access are granted or terminated on a “need-to-know basis related to the performance and fulfillment of the user’s current responsibilities,” which is precisely what NIST suggests for
managing accounts (The State University of New York at Canton, n.d.). Furthermore, it goes on to acknowledge that “as these responsibilities evolve, the authorization will change as appropriate” (The State University of New York at Canton, n.d.). This requires that SUNY Cantons’ IT department routinely monitors account privileges, benefiting their organization by ensuring users have correct privileges even over time.

SUNY Binghamton’s information security policies do not mention the principle of least privilege. Regarding access control, their Information Security Program mentions that there is a User Management Process established by the University that outlines, identifies, and manages user functions to “ensure that only authorized individuals have access to University applications and information and that these users only have access to the resources required for authorized purposes” (Binghamton University State University of New York, 2017). It goes on the explain the sub-processes of the User Management Process, which include granting, removing, and a periodic review of “privileged accounts” to a user. While there is no mention of implementing the principle of least privilege, they do a satisfactory job addressing PR.AC-4, concerning access permissions and authorizations.

**Recommendations & Conclusion**

The objective of this study was to establish if SUNY computer policies adequately addressed human error. Another aim was to examine if SUNY Albany users are receiving education or training on Cybersecurity. The outcomes of this study indicated that SUNY Albany, SUNY Canton, and SUNY Binghamton have computer use policies that sufficiently address human error compared to NIST’s Cybersecurity Framework V1.1 Core subcategories selected. Due to the select categories chosen, further examinations should be completed to identify more
specifically where these policies are lacking. Originally, it was thought that these policies would insufficiently address human error.

There are two areas of recommendation for the universities: policy and training. Policies are an essential part of organizations because they provide a system for everyday operations. By having high-quality, relevant, well disseminated, and well-understood policies, the universities can better protect themselves against cyber-attacks stemming from human error. The other portion of recommendations, training, is equally important because the universities’ policies call for user training.

Regarding the policies reviewed, the information security policies and computer access policies established by the SUNY system, SUNY Albany, SUNY Binghamton, and SUNY Canton do a satisfactory job addressing NIST’s subcategories in NIST Cybersecurity Framework. There are many more subcategories that their policies can be evaluated against, so it would be ideal for each institution to review the remaining subcategories relevant to the University’s needs. The policies can have a human-centric or a more technological approach. The human-centric policies should be geared towards training and behaviors, while the technological policies should complement the training and enforce what is being taught.

The SUNY Information Security Policy requires that SUNY institutions provide annual training to “all individuals who access State University information assets and systems” (The State University of New York, 2016). From this research, we can confirm that SUNY Albany implements yearly training for faculty. However, its effectiveness is uncertain due to the negative reviews. One way to better secure SUNY information and assets is to implement more specific requirements for the local campus policies and investigate how beneficial the policies are.
Some examples of human-centric safeguards that can be made into policies and procedures range from positive reinforcements for good behaviors, and basic awareness campaigns, to the threat of termination for bad behaviors. If there is no incentive to comply with the procedures and retain the information from the training, then the number of attacks deriving from human error will continue to rise. More specifically, some policies could call for the creation of security checklists, “making policies and procedures high-profile, creating explicit disciplinary measures for lax security practices and even raising the threat of litigation as measures that can be taken to encourage or coerce people into better security practices” (Coffey, 2017). Additionally, Coffey suggests awareness campaigns that would elevate the general knowledge of information security and safety.

As for training, some ways to improve security awareness are using modeling and simulations, gamification, and periodic review of best practices for end-users. Niazi explains that using modeling and simulations can improve research by developing and implementing new techniques, tools, and strategies. Furthermore, modeling and simulation can be used when real experimentation is not convenient, dangerous, or not cost-effective (Niazi, 2019). Gamification techniques in training would help keep the end-user motivated and engaged and can enhance the learning experience by making lessons more enjoyable, more interactive and allowing users to see real-world applications. Gamification in training that uses rewards and positive reinforcement would raise end-user interest and participation and ultimately elevate the effectiveness of the training.

Another aspect of security awareness is the institution’s culture. SUNY Universities should build an institution-wide culture and participation where decision-making and application of Cybersecurity best practices develop into daily pursuits for end-users at all levels (Khader et
Implementing a culture of cyber awareness helps users learn to understand their role in keeping their information safe. Changing a culture is a very difficult process. It is also suggested that upper-level management communicate the value and purpose of cybersecurity education before implementing training and upholding the practices that they are enforcing on the end-users. Understanding the value and purpose of the training makes the learning more meaningful and makes the users more likely to pay attention because they are aware of what is at stake.

Lastly, SUNY Universities can maintain awareness of Cybersecurity best practices for end-users by revisiting topics regularly and incorporating ongoing awareness activities; without reinforcement, the institution must regularly rebuild rather than build upon them (Khader et al., 2021). By reinforcing Cybersecurity best practices for end-users, institutions can build upon what they already have, rather than having to constantly rebuild. This will help advance the training and security of the information and data overall.

In conclusion, SUNY institutions have policies that show they are aware of the importance of information security and human error. The implementation of the policies and the awareness of end-users must be reviewed in more depth to fully understand how functional and worthwhile the policies are. Additionally, the training mentioned in the policies should receive more attention because it is a crucial part of mitigating cyber-attacks stemming from human error. The reviewed policies fare well against the part of the NIST framework utilized in this research. However, due to the limited subcategories assessed, these policies would benefit from further examination of a more in-depth comparison to the entire NIST framework. Furthermore, surveys tailored to a university’s faculty or students specifically would yield data that is more indicative of that group’s security awareness. The human factor is becoming increasingly
important for an organization’s cyber defense due to human error being a primary reason for security breaches. For future cybersecurity research, there must be a shift from focusing on the technical aspect to the human aspect to prevent the frequent occurrence of successful cyber attacks.
References

https://www.binghamton.edu/its/about/governance/policies/comp-net-usage-acceptable-use.html

https://www.binghamton.edu/its/about/governance/policies/data-security-guidelines.html

https://www.binghamton.edu/its/about/governance/policies/info-security.html

https://www.binghamton.edu/operations/policies/policy-301.html


http://dx.doi.org/10.6028/NIST.SP.800-53r4


https://doi.org/10.4108/trans.sesa.01-06.2013.e2


https://doi.org/10.2478/hjbpa-2018-0024


https://www.suny.edu/sunypp/documents.cfm?doc_id=583


https://www.suny.edu/sunypp/documents.cfm?doc_id=848


https://www.suny.edu/sunypp/documents.cfm?doc_id=890
The State University of New York at Canton. (n.d.) *Computer and network use policy.*

https://www.canton.edu/policies/procedures/admin/computer-use-policy/

The State University of New York at Canton. (2021). *Faculty handbook.*

https://www.canton.edu/media/pdf/faculty_handbook.pdf


https://www.albany.edu/undergraduate_bulletin/cehc_courses.html


https://www.albany.edu/facets/news/2021-cybersecurity-training-faculty

University at Albany State University of New York. (2021). *Information security.* Ask IT. Retrieved February 20, 2022, from

https://wiki.albany.edu/display/public/askit/Information+Security


https://www.albany.edu/risk-management-compliance/policy/information-security