ADOPTION OF ARTIFICIAL INTELLIGENCE-BASED CYBERSECURITY TOOLS AT GEORGIA'S TWO-YEAR COLLEGES

by

MICHAEL CLOUGH

B.S, Macon State College, 2007

M.S, Columbus State University, 2010

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements of the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2025

Adoption of Artificial Intelligence-based Cybersecurity Tools at Georgia's Two-year Colleges

Michael Clough, *Middle Georgia State University, michael.clough@mga.edu*

Abstract

Two-year public colleges in Georgia face significant challenges in maintaining robust cybersecurity programs with limited resources, especially as regulatory demands continue to rise. At the same time, advancements in artificial intelligence (AI) and machine learning (ML) present new opportunities to enhance threat detection, compliance management, and policy development. However, little is known about how these institutions adopt AI-based cybersecurity tools, the barriers they encounter, and the perceived benefits or drawbacks of integrating such solutions. This phenomenological qualitative study explores the lived experiences of information technology (IT) leaders at Georgia's two-year colleges as they implement AI-enhanced cybersecurity products. Semi-structured interviews investigate how these leaders perceive the effectiveness and efficiency of AI-driven tools, particularly in automating repetitive tasks, prioritizing critical threats, and creating tailored policies and procedures. The research also examines the potential of generative AI to assist in policy development for staff members with minimal formal cybersecurity training. The study seeks to illuminate both the promises and pitfalls of AI adoption in resource-constrained educational environments. Insights gleaned may inform best practices, guide institutional decision-makers, and support other higher education entities aiming to optimize AI-based cybersecurity solutions while adhering to evolving regulatory requirements.

Keywords: Cybersecurity, Artificial Intelligence, Higher Education, Information Technology

Introduction

Many of the two-year colleges in Georgia have Information Technology (IT) departments that would be considered small compared to their four-year college counterparts. These staff are often tasked with multiple roles and job duties. Frequently, these staff members do not have formal cybersecurity training but are required to maintain the college's cybersecurity program. Studies have found that specialized training in cybersecurity is necessary (Liu et al., 2020). On top of their regular day-to-day duties, these staff members face ever-increasing regulatory scrutiny (Fair, 2022; *Family Educational Rights and Privacy Act: Guidance for School Officials on Student Health Records | Protecting Student Privacy*, 2023; McIntosh, 2022). These IT departments are not seeing increased budgets to assist with the additional cybersecurity requirements but instead have to find ways to improve efficiency. Additionally, IT departments need to find ways to offload mundane and repetitive tasks so that they have more time to focus on analyzing problems and critical tasks.

New and existing cybersecurity tools integrate artificial intelligence (AI) and machine learning (ML) technologies to increase their effectiveness and efficiency (Kaur et al., 2023). Studies in disciplines outside of IT have shown that tools utilizing AI can improve the accuracy of detection, which in turn will increase efficiency (Dy et al., 2024). Offloading detection and prioritizing critical attacks will also allow IT departments to spend time and resources defending against those attacks that would have caused the most damage to systems.

Generative AI has been shown to increase the speed, comprehensiveness, and rigor when creating policies and procedures by bringing in data from many sources (Patel et al., 2021). Generative AI could assist IT departments with tailoring policies and procedures that fit their environment, shortening the typical cycle of reviews and approvals. However, with the current perception of AI, human interaction would still need

to be present, as AI does not currently have compassion or empathy (Wirjo et al., 2022). Even with this perception and additional review, increased efficiency and tailored policies and procedures would allow the IT departments more time to focus on the critical workload and not spend time creating these policies from scratch.

AI-based tools have been shown to enhance cybersecurity programs, but there is a limited understanding of their impact within these institutions. The lack of comprehensive data on how these colleges integrate AI technologies, tied with potential barriers such as resource constraints and lack of formal training, hampers their ability to protect sensitive information and maintain secure digital environments. This study seeks to address the gap in understanding how Georgia's two-year colleges integrate AI-based cybersecurity tools and the challenges they face to improve the effectiveness of these technologies in securing institutional data and maintaining compliance.

This study examines the adoption of AI cybersecurity tools within Georgia's two-year colleges by assessing how these institutions integrate AI technologies into their cybersecurity practices and identifying the challenges and benefits associated with their implementation. Through a qualitative analysis, this research seeks to provide insights into the perceived effectiveness and increased efficiencies of AI-based cybersecurity tool usage in two-year colleges. Additionally, this study aims to gain insight into any perceived effectiveness of utilizing generative AI to assist in creating effective policies and procedures for IT staff with little to no formal cybersecurity training.

RQ1: How have artificial intelligence-based cybersecurity tools been adopted in higher education, particularly within two-year colleges, and what are the documented impacts, challenges, and benefits of these integrations?

RQ2: What is the perception of generative AI being utilized to create effective cybersecurity policies and procedures for IT staff with minimal formal training?

This study aims to understand the perceptions of the IT leadership who have integrated these technologies into their organization and their feelings on the overall effectiveness of these tools. It will explore their views on the perceived effectiveness of these tools, particularly in enhancing operational efficiency and maintaining compliance with evolving regulatory requirements. Additionally, the findings may offer valuable insights for other educational institutions, government agencies, and non-profit organizations planning similar technology integrations.

Literature review

As Artificial Intelligence (AI) and machine learning (ML) technologies are integrated into more cybersecurity products, the staff in information technology (IT) departments can no longer ignore AI and ML technology. While legitimate security companies are incorporating AI and ML, so are the attackers, making it much more difficult for IT staff to manually remediate, protect against, and keep current on the threats being used today (Chang et al., 2023). Further complicating the problem is that the allocated budget for two-year public colleges in Georgia is much less than that of their four-year colleges and university counterparts. However, the literature lacks a thorough exploration of how these financial constraints impact the ability of two-year colleges to adopt and sustain AI-based cybersecurity tools, making this an area that requires a more profound understanding.

Cybersecurity tools

According to Grajek (2022), cybersecurity was the top IT issue faced by higher education institutions. Grajek further called for building processes and controls that strengthen the protection of student data

because cybersecurity threats were more difficult to recognize and detect. Researchers have proposed that AI and ML technologies are one way to improve the detection of these new threats (Mahfuri et al., 2024). The tools that include these technologies have been shown to detect patterns and identify anomalies better than existing tools while also categorizing and prioritizing events (Mahfuri et al., 2024; Watkins, 2024). Additionally, they can search extensive data sets to speed up the identification of new patterns. Current cybersecurity tools increasingly include AI and ML technologies in their product lines. Cybersecurity tools that integrate this technology suggest that by including these technologies, the efficiency of the products increases, is more effective than humans, and allows IT staff to focus on critical tasks (Raimundo & Rosário, 2021). Companies like CrowdStrike and IBM have produced case studies showing how the use of their tools has reduced threat detection time, reduced overall costs, and provided more timely information to IT staff than the manual processes that were being performed (Dickson et al., 2023; *Securing a Global Solutions Landscape*, 2024). Other cybersecurity tools, including Darktrace, Cylance, CrowdStrike, Cylance, FireEye, Proofpoint NexusAI, and IBM Watson for Cybersecurity, integrate with Artificial Intelligence to perform various analyses of email, endpoints, networks, and user anomaly detection (Mahfuri et al., 2024; *NexusAI - AI Machine Learning & Cybersecurity | Proofpoint US*, 2021; *The CrowdStrike Falcon® Platform*, n.d.).

AI and ML can be used for more than detecting threats and abnormal behavior. These tools can additionally be used to perform vulnerability analysis and remediation, configuration management, and automated policy enforcement (Kaur et al., 2023; Mahfuri et al., 2024). Automating the remediation of vulnerabilities can reduce the burden on small IT departments. These tools can assist in prioritizing the vulnerabilities that need to be remediated and could group the vulnerabilities that require manual intervention with those that can be automated, according to Kaur et al. (2023), these tools can identify the potential attack vectors for a successful exploit based on publicly available datasets to assist with prioritizing threats.

There is a limited understanding of how these tools are integrated into two-year colleges. Many studies focus on the general capabilities of the tools rather than the practical challenges and experiences faced by institutions with limited budgets.

Compliance and Governance

Two-year public colleges must comply with the laws and regulations because they accept Federal Title IV funding for student financial aid (Family Educational Rights and Privacy Act: Guidance for School Officials on Student Health Records | Protecting Student Privacy, 2023; The Gramm-Leach-Bliley Act (GLBA), n.d.; Grama, 2020). These federal funds require two-year public colleges to implement cybersecurity programs that protect student data. Additionally, many of these institutions must be regularly audited for compliance and provide audit reports to accrediting agencies.

FERPA and GLBA are two of the primary laws impacting the college's compliance and governance members most, as failing to comply can result in personal legal ramifications and potential loss of funding and accreditation. GLBA prescribes rules that require a college to develop a cybersecurity program based on a risk management approach like a financial institution. Additionally, FERPA covers students' educational records and ensures they are adequately protected. Both laws require specific steps to be enacted whenever a data breach occurs to ensure students can protect their data from being misused.

Following the laws that a two-year college must follow requires proper information technology governance. Without this governance, compliance is not easily obtainable. Governance extends beyond the information technology division and must include users from other departments. Without involving other divisions, a clear picture of the risk to the higher education institution cannot be fully known (Bamber, 2023). Once the risks are understood, policy and governance can be implemented to mitigate them and protect student data appropriately.

Compliance within GLBA requires a risk assessment of all systems that could store or process financial data (Enforcement of Cybersecurity Requirements under the Gramm-Leach-Bliley Act, n.d.; Grama, 2020). While FERPA does not explicitly require a risk assessment, completing one for systems containing student information will ensure that the risks associated with those systems are understood and can be adequately protected. Risk assessments are vital for the institution as they are an essential first step in organizational governance and compliance.

Two-year colleges in Georgia that fall under the executive branch of the State of Georgia must also follow the policies, standards, and guidelines of the State of Georgia's agency named Georgia Technology Authority (GTA). This agency has provided additional steps for implementing AI-containing software. The colleges must seek approval from GTA to implement AI-based software and develop additional compliance steps that entail monitoring the software, training users, and eliminating bias from the software (*Artificial Intelligence Responsible Use*, 2023; *Enterprise Artificial Intelligence Responsible Use*, 2023).

A Study by Kaczorowska-Spychalska et al. (2024) found that Generative AI can be used to make better-informed business decisions. When used legitimately and ethically, these business decisions can be used to create policies and procedures supporting the business. Additionally, the users creating policy can increase the speed and efficiency of the policy process by using AI to analyze datasets and develop policies that will support the business based on identified patterns (Patel et al., 2021; Wirjo et al., 2022). AI can also provide evidence-based insights when creating policies to identify the correct business risk.

It has been found that AI can be used to automate tasks during the risk assessment process (Kaur et al., 2023). These automated tasks can then feed data back to the users to aid in risk planning and to assist the planner in making more informed business decisions. AI tools have been shown to aid in governance; however, the research does not examine how a two-year college can utilize these tools to maintain compliance and support governance.

Higher Education and budget challenges

Higher Education Institutions differ from most organizations due to challenges like decentralized IT, academic freedom, open access, and shared governance (Alexei, 2021; Kam et al., 2022; Sander, 2023). Additionally, the leadership in higher education often does not place cybersecurity high on the list of the organization's values. It has been found that higher education institutions typically respond better to flexible approaches to policy and procedures as opposed to the more rigid approaches found in most private organizations (Kam et al., 2022). Flexibility promotes collaboration and teamwork and, in turn, causes peers to perceive the importance of cybersecurity. Also, the flexible approach aligns closer to the culture within most higher education institutions. Kam et al. (2022) also proposes that not sanctioning employees for cybersecurity mishaps will further improve the organization's security posture.

The cost of a data breach has increased over the last several years for a cybersecurity incident. Studies have also shown that cybersecurity incidents in higher education take longer to recover compared to other industries (Sander, 2023). Several organizations in the education industry have published basic incident response planning guidance for higher education institutions. These strategies include what to do before, during, and after an incident. The typical steps that all of these strategies suggest include items such as developing an incident response plan and team, remediation and reporting to appropriate agencies, and doing post-incident analysis (Cybersecurity Incident Planning for Institutes of Higher Education, n.d.; Sander, 2023; Whalley et al., 2024). Also, research has shown that risk management frameworks could improve the posture of higher education institutions. Different regulations often require these frameworks. Selecting one that best fits the organization will simplify implementation and compliance, as improperly applying the framework could cause more problems than doing nothing (Alexei, 2021).

Comparing the allocated budgets of the four-year public colleges and the two-year public colleges in Georgia, there is a wide gap between the budget allocation per student. According to the Governor's Budget Report for AFY 2024 (*Governor's Budget Reports | Governor's Office of Planning and Budget*, n.d.), the four-year colleges received a total of $9.072 Billion in FY23, as opposed to the two-year colleges, which only received $1.098 Billion. Enrollment for the four-year colleges during the same timeframe was 344,392 students (*University System of Georgia Enrollment Hits Record High of 344,392 | Communications | University System of Georgia*, n.d.); for the two-year colleges, enrollment was 136,114 (*Enrollment & Graduates – TCSG | Technical College System of Georgia*, n.d.). For FY23, the budget per student for four-year colleges was $26,342; for the two-year colleges, it was only $8,067. By comparing these budget numbers, the researcher can see that two-year colleges do not have the budget to devote to cybersecurity tools, staff, or training.

AI Implementation Challenges

Implementing AI has several challenges and limitations, with the most prevalent issue being that the AI and ML models need to be as fair and bias-free as possible (Alier et al., 2024; Ejreaw & Annowari, 2023; Wirjo et al., 2022). If the models used are not fair and bias-free, the decisions may be skewed and unfair to specific populations, anomalous behaviors could be missed, or new threats could go unnoticed. Additionally, by interacting with AI, any data entered may be used in future data sets to train future models (Alier et al., 2024). Colleges must know that collecting or entering sensitive or protected data into an AI tool could violate privacy laws and regulations.

Research by Ejreaw and Annowari (2023) has found that AI is acceptable for automating tasks, but human judgment should still be used to interpret the results. They reported this because many AI systems are considered "black boxes," with the models not being fully understood or open for others to review. Ryzheva et al. (2024) have discussed how AI has not yet been created to handle every task a person may do; instead, it is limited to being good at specific tasks only. The lack of training on role-specific competencies is required to integrate AI and ML within cybersecurity (Cusak, 2023). Without these skill sets, AI and ML are underutilized and not embraced by current IT departments. This highlights a critical area that needs further examination on how IT departments in two-year colleges can better develop and leverage AI skills.

Research Methodology

This study employs a phenomenological qualitative research design to explore the experiences of information technology leadership at Georgia's two-year colleges. The phenomenological qualitative research approach is well-suited for this research, as it seeks to understand the experiences of these individuals as they lived and worked through the paradigm shift of using software that began implementing artificial intelligence and machine learning tools in cybersecurity and the implementation of this software at their organization (Creswell & Creswell, 2018; Moustakas, 1994).

Participants

According to Creswell and Poth (2018) five participants would provide the needed data saturation for this study if a purposeful criterion sampling strategy were used. The purposeful strategy the researcher used to develop the sample focused on participants over 18 years old, currently working at a two-year college, a leader in information technology at their college, and someone who worked with products containing artificial intelligence. Leaders in information technology included the Director of Information Technology, VP of Information Technology, Chief Information Officer, and other positions with managerial oversight of other employees.

Interview questions

The researcher could not find previous studies with published interview questions on artificial intelligence focusing on cybersecurity and operational information technology. The researcher developed questions for a pilot study focusing on the use of artificial intelligence in cybersecurity and operational information technology.

Procedures

The researcher obtained Institutional Review Board (IRB) approval to interview human subjects. Once completed, the researcher also needed to obtain permission from the college's parent agency and each college president. The researcher contacted twenty colleges within the Technical College System of Georgia (TCSG) to ensure that the researcher had access to adequate participants. The colleges in this system can grant associate degrees, diplomas, and certificates that can be completed in two years or less. The researcher used the college's online directory to find individuals who fit the purposeful sampling as best as possible and recorded their names and email addresses. Once the researcher received permission from the first ten colleges, the researcher contacted those colleges' information technology leadership through email, looking for volunteers to participate in the interviews. The researcher had eight participants volunteer in a sufficient timeframe for the interview but only scheduled interviews with the first six participants because data saturation was achieved, and no new themes or insights were gained. The following table shows the response rate of interview requests sent, approved, or denied.

Table 1

Interview Request Response Rate

Description	Quantity
Interview Request Sent	20
Approved	15
Denied	1
No Response	4

A semi-structured interview protocol was used as a way to guide the interviewees and also allow them to provide insights into their experiences using artificial intelligence and machine learning-based cybersecurity tools (Creswell & Poth, 2018; Terrell, 2016). Additionally, this type of interview protocol allowed the interviewee to explain their use of Generative AI. The interviews were conducted using web conferencing software to perform a 30 to 45-minute interview with individuals from different areas of Georgia and reduce the burden of traveling for the researcher and the participants. Additionally, the web conferencing software produced an initial transcription of the interview. The researcher then manually reviewed and edited the transcription for accuracy.

Utilizing the modified Stevick-Colaizzi-Keen method described by Moustakas (1994) the researcher read the transcriptions several times to understand the participants' experiences and gain initial insights into how the participants felt about artificial intelligence. Using Delve: Qualitative Data Analysis Software, the researcher used these initial insights to begin relating and clustering the texts into themes. This software allowed the researcher to refine the themes further to understand the essence of the lived experiences. The researcher repeated this process for each participant to enhance and build a description of each theme that arose. Through the participants' accounts, the analysis provides insight into the practical application of AI implementation in higher education cybersecurity.

Results

This research analyzed the results of six interviews with the selected participants. The following table shows demographic information of the six participants.

Table 2

Demographic information of participants

Description	Group	Quantity
Size of College (number of students)	< 3000	3
	3000-6000	1
	> 6000	2
Education		
	College	2
	Graduate School	4
Age		
	< 40	2
	> 40	4
Sex		
	Male	6
	Female	0
Work Experience (Years)	< 20	2
	> 20	4
Department Size (No. of Employees)	< 10	4
	> 10	2

After analyzing the interviews, four themes emerged: (1) Incremental and Reactive AI adoption, (2) Operational Efficiency vs Administrative Challenges, (3) Privacy Concerns, Trust Issues, and Skepticism, and (4) Barriers to Institutional Integration. These themes answer the research question by explaining the adoption of cybersecurity tools and their impacts, challenges, and benefits. Additionally, the participants explained their perceptions of generative AI being used to create policies and procedures.

Incremental and reactive AI adoption

Many participants expressed how a vendor or software developer implemented artificial intelligence integrations as part of a larger package. However, they were not explicitly purchased because they contained artificial intelligence features. Anti-malware and spam filtering tools were discussed as examples of how artificial intelligence components were added after purchasing the software as an included feature upgrade. One participant mentioned how “there wasn’t a lot of direct interaction with the AI components.” Another participant mentioned, “When it comes to AI implementations that coexist with a product, you are not actually implementing AI.”

The participants regularly did not know products even contained AI because of the incremental changes to the product by replacing non-AI components with upgraded AI components. One example mentioned was Microsoft Word; while not typically considered a cybersecurity tool, it is used for policy writing; the spelling and grammar check features now rely on AI to offer better and more accurate suggestions. The

participants used statements like “wild wild west,” “grassroots’, and “shadow IT” when describing how members of their faculty and staff were adopting AI tools.

Several participants mentioned how the changes and reactive adoptions cause compliance issues with the colleges' governing agencies because colleges must report and get approval for AI-containing software. One participant mentioned how they “provide those lists to our supervising system” but are still awaiting approval for software their faculty and staff have already been actively using.

Operational efficiency vs administrative challenges

Adopting AI-based cybersecurity tools varied significantly, with most colleges integrating AI passively as part of a vendor's solutions. The participants mentioned that much of the AI works in the background, and you do not have to interact directly with the features. One participant described a security event and how the endpoint detection and response (EDR) solution triggered an alert and stopped an attempted system compromise. This participant expressed how, without the software, their staff was not trained to spot this type of event and most likely would have led to an even more significant event had the software not stopped it. Another participant expressed how the same EDR software triggers false positives regularly. The participant stated that they noticed “a few false positives. When we are installing upgrades, or we’re deploying new software, it would think it is something malicious where, in fact, it was something intentional.” The participant explained how time would have to be spent investigating to ensure it was a false positive and then working with the vendor to allow the intentional action.

Additionally, many participants expressed how generative AI, such as ChatGPT, Google Gemini, etc, was helpful with day-to-day tasks. Participants used statements like “it completes my sentences,” “getting the good summary of what the web says about things,” and “do a summary of a meeting, and that really worked out well.” One participant explained how they used generative AI to change the reading level of an email he crafted for students about phishing awareness because, in previous semesters, they had high rates of student email compromise. He explained how “from a cybersecurity perspective and, all the information was accurate,” and he felt the email “was easily digestible” compared to his previous emails.

Privacy concerns, trust issues, and skepticism

All participants shared concerns about student data privacy and trust that AI was not incorrectly using or storing sensitive data. Participants used words like “trust,” “scared,” “suspicious,” and “worried” when discussing student data and AI. Additional words can be seen in Figure 1. A table showing additional words and the total count used by participants can also be found in Figure 2.

Figure 1

Word cloud of feelings related to AI

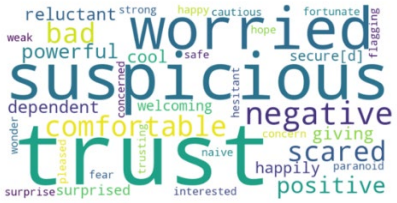
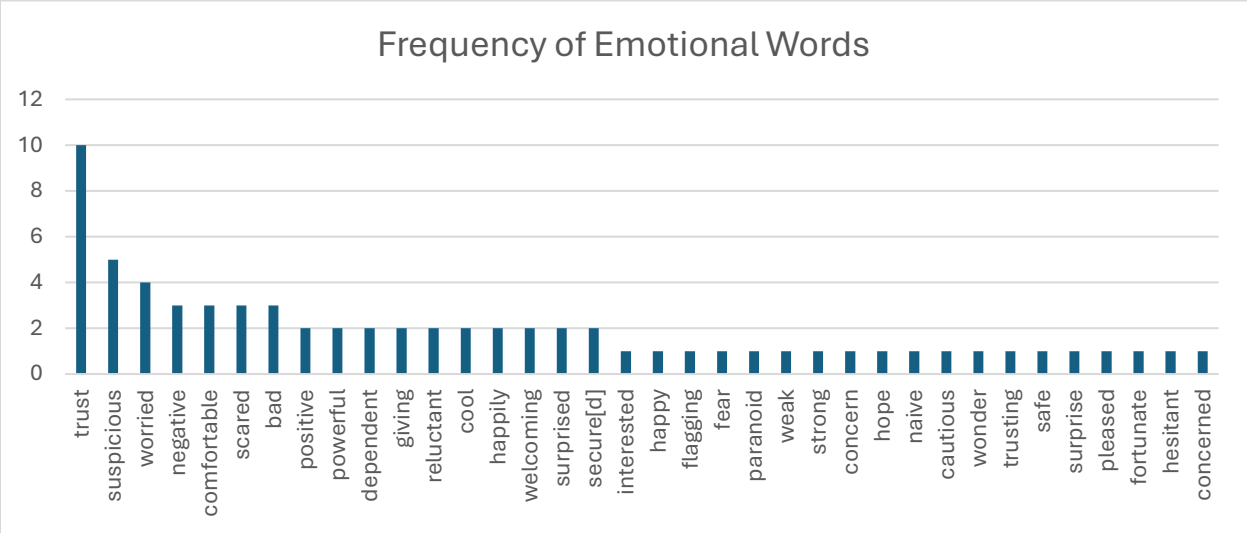


Figure 2

Frequency of Emotional Words



One participant discussed how "as a state agency, GTA has made it clear that we are not supposed to be putting production information or production data into a large language model AI tool." Another participant said, "There could be negative implications because what if somebody puts in a student's PII information into that tool and then [redacted] uses it to learn, … that is something we have to be very careful of." Furthermore, a third participant shared similar concerns:

> The biggest thing I would be worried about is how it is learning about our environment and where it is storing the information that it is learning because it could get very risky if all that data is constantly learning about us gets compromised or gets leaked out there in the wild somewhere.

When discussing the use of generative AI in policy development, one participant said, "I'm a little bit suspicious, so I'm very careful what I've put in…if I'm trying to come up with a policy for a particular subject…I may be very vague." Another participant said "I'm just scared that I would miss something. ChatGPT would miss something."

Participants later discussed how they were concerned that generative AI tools would not be effective in creating policies for their college because they would have to redact information when prompting the generative AI tool, and then returned information would not be relevant.

Barriers to institutional integration

Many of the participants discussed how being a state agency, they were required to follow the rules of several outside agencies, which required approval from those outside agencies. One participant noted that the rules "doesn't mention any grandfathered-in software packages," which had caused some confusion on what is allowed and not allowed to be used because many participants noted several AI-based tools in use before the rules were published. Another participant said, "we are waiting for…more directives coming from [redacted], before we really jump into anything officially."

The participants discussed how they would choose software that contained AI because, as one participant noted, "at this point, I think everyone should be using it to a degree." Many participants discussed how the

faculty and staff at their college had already started using AI-based tools independently without help from the participants' departments.

One participant questioned that implementing AI would increase the cost of products by saying, “How is AI gonna increase the cost of these tools right now?”

Discussion

The interviews revealed that AI-based cybersecurity tools in two-year colleges were often embedded in previously implemented vendor solutions or added as a feature upgrade to an already deployed product. This led to the reactive adoption of these tools. Participants also noted how individuals outside their department successfully utilized AI-based products with minimal IT intervention. The participants acknowledged the benefits but also identified concerns over privacy, data security, and compliance gaps due to changing regulations from other intergovernmental agencies.

These results bolster existing research indicating the concerns of privacy and data security due to the lack of transparency of the AI algorithms (Ejreaw & Annowari, 2023; Kaur et al., 2023). This lack of transparency caused many of the IT leaders not to feel comfortable providing access to systems that contain sensitive data to AI-based cybersecurity tools. The compliance risk of unintentionally disclosing student data to generative AI tools is an additional fear for many participants, as GLBA and FERPA do not allow disclosure of this type of data (*Family Educational Rights and Privacy Act: Guidance for School Officials on Student Health Records | Protecting Student Privacy*, 2023; *The Gramm-Leach-Bliley Act (GLBA)*, n.d.).

Additionally, the interviews reinforce existing research on how AI-based cybersecurity tools used in conjunction with human operators provide better decision-making processes and operational efficiencies (Kaczorowska-Spychalska et al., 2024; Kaur et al., 2023; Raimundo & Rosário, 2021). These tools allow users to analyze threats and make decisions faster, but a human review is often needed to ensure the accuracy of the decision (Mahfuri et al., 2024).

The participants did feel that using generative AI to create cybersecurity policies would not be beneficial as the policies would not be tailored for their environment, provide expert analysis of regulation, and may unknowingly show bias towards groups of individuals, which agrees with previous research (Patel et al., 2021; Wirjo et al., 2022)

While none of the participants directly mentioned the recent incident with cloud-based AI and Large Language Model (LLM) provider Snowflake, the breach was recent enough that it could have influenced the participants (*The Snowflake AI Data Cloud*, n.d.; *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, 2024). This incident highlighted how sensitive data stored for training AI models could be accessed by malicious actors and cause reputational harm to the companies using the service.

This study found that the participants were cautious regarding AI due to the limited information available on the algorithms and data usage of AI-based tools. However, many participants understood that AI-based tools were already available and used by their institutions, students, and malicious actors and should not be ignored.

This study did have several limitations. One of the study's limitations is that the researcher is a member of the information technology leadership at one of the two-year colleges and previously worked for the college's parent agency in a role where participants directly interacted. Survey participation was voluntary,

and participants were selected on a first-come, first-served basis; as such, the volunteers were all males from rural areas of Georgia. Future studies should include a more diverse population of participants from different geographic regions.

Future research should be conducted on similar colleges in different areas to understand if the geographic area will affect the results. This study could be expanded to non-government organizations (NGOs) and other non-profit organizations to understand the perceptions of AI-based cybersecurity tools on those organizations, as these organizations are known to have small IT staffs and operating budgets similar to those of the selected college system.

The existing research on AI tools provided results similar to those presented in this study. Most participants understood the helpful nature of AI and often stated how it benefited both themselves and others. The participants discussed how they used generative AI personally outside of work but were cautious about using it for work-related tasks because they did not want to present data that may disclose information about the systems they managed or disclose sensitive data. All participants were cautious about AI because of the lack of available information on how the collected data was used and if it would be later used to train future AI or ML tools. Not knowing how the data is stored or used could cause compliance issues. The existing research also validates how human oversight is needed when using generative AI to review the output and provide more applicable results.

Conclusion

Integrating Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity tools could revolutionize how IT departments in higher education, particularly in two-year public colleges, handle security threats. AI and ML have shown immense potential in enhancing threat detection, automating responses, and managing vulnerabilities. As cybersecurity becomes more complex and critical issues are constantly found, these technologies offer efficient solutions. Given the budget constraints faced by two-year public colleges in Georgia, this is crucial. Two-year public colleges in Georgia face unique challenges due to significantly lower budgets than their four-year counterparts. Adopting AI and ML technologies can help bridge this gap by providing cost-effective and efficient solutions to enhance the college's cybersecurity posture. By leveraging AI, these institutions can improve their threat detection capabilities, ensure compliance with regulations, and manage their cybersecurity risks more effectively.

Compliance with federal regulations such as FERPA and GLBA is a significant concern for two-year public colleges, as failure to comply can lead to severe consequences, including legal ramifications and loss of federal and state funding. AI can play a pivotal role in ensuring compliance by aiding in developing cybersecurity programs that protect student data. It can help automate risk assessments, providing a clearer understanding of potential threats and ensuring appropriate measures are in place to mitigate them. The participants mentioned waiting on rules and policies from parent agencies that were not reactionary before further using and implementing AI-based tools.

Despite the benefits, implementing AI in cybersecurity is not without challenges. Data privacy is a main concern, as AI systems can potentially use entered data to train future models, which might conflict with privacy regulations. Moreover, while AI can automate many tasks, human oversight remains essential to interpret AI-generated results and make informed decisions, especially given that many AI systems operate as "black boxes" with limited transparency. This limited transparency causes distrust of many AI platforms as the individuals using the software are not privy to how the training data is stored or used across the platform.

The colleges implementing and using AI-based cybersecurity tools need the tools to be more transparent and provide clear descriptions of how data is used and if the data collected is used to train future models.

The transparency will provide the compliance information required by GLBA on third-party vendor risk management requirements. Additionally, providing this transparency will ease the fear of AI.

Integrating AI and ML into cybersecurity is a technological advancement and a necessary evolution in response to increasingly sophisticated threats. Threat actors have already adopted AI to aid in performing malicious activity, and as such, two-year public colleges need to combat this activity by utilizing similar technology. Adopting these technologies for two-year public colleges in Georgia can boost their cybersecurity defenses despite budget constraints. As these technologies evolve, they promise to create more secure and resilient educational environments, protecting both institutions and their students.

References

Alexei, A. (2021). Cyber Security Strategies for Higher Education Institutions. *Journal of Engineering Science (Chişinău)*, *XXVIII*(4), 74–92. https://doi.org/10.52326/jes.utm.2021.28(4).07

Alier, M., García-Peñalvo, F.-J., & Camba, J. D. (2024). Generative Artificial Intelligence in Education: From Deceptive to Disruptive. *International Journal of Interactive Multimedia and Artificial Intelligence*, *8*(5), 5. https://doi.org/10.9781/ijimai.2024.02.011

Artificial Intelligence Responsible Use. (2023, December 12). https://gta-psg.georgia.gov/psg/artificial-intelligence-responsible-use-ss-23-002

Bamber, C. (2023). Exploring Enterprise-Wide Risk Management System in Higher Education: Management Dynamics in the Knowledge Economy. *Management Dynamics in the Knowledge Economy*, *11*(3), 267–285. https://doi.org/10.2478/mdke-2023-0017

Chang, J., Li, Z., Kaveh, M., Zhang, Y., Li, J., & Yan, Z. (2023). A Survey on AI-Enabled Attacks and AI-Empowered Countermeasures in Physical Layer. *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*, 1–7. https://doi.org/10.1109/WF-IoT58464.2023.10539554

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (Fifth edition). SAGE.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (Fourth edition). SAGE.

Cusak, A. (2023). Case Study: The Impact of Emerging Technologies on Cybersecurity Education and Workforces. *Journal of Cybersecurity Education, Research and Practice*, *2023*(1).

Cybersecurity Incident Planning for Institutes of Higher Education. (n.d.). United States Department of Education. Retrieved February 19, 2024, from https://fsapartners.ed.gov/sites/default/files/2023-02/FSA_IHEIncidentPlanning_508.pdf

Dickson, F., Kissel, C., & Marden, M. (2023, November). *IDC Study: The Business Value of the CrowdStrike Falcon Platform*. https://crowdstrike.com/explore/business-value-of-crowdstrike/

Dy, A., Nguyen, N.-N. J., Meyer, J., Dawe, M., Shi, W., Androutsos, D., Fyles, A., Liu, F.-F., Done, S., & Khademi, A. (2024). AI improves accuracy, agreement and efficiency of pathologists for Ki67 assessments in breast cancer: Scientific Reports. *Scientific Reports*, *14*(1), 1–12. https://doi.org/10.1038/s41598-024-51723-2

Ejreaw, A. M. A., & Annowari, N. B. (2023). Artificial Intelligence in Cybersecurity: Opportunities and Challenges. *International Journal of Business Society*, *7*(6).

Enforcement of Cybersecurity Requirements under the Gramm-Leach-Bliley Act. (n.d.). Retrieved April 21, 2024, from https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2020-02-28/enforcement-cybersecurity-requirements-under-gramm-leach-bliley-act

Enrollment & Graduates – TCSG | Technical College System of Georgia. (n.d.). Retrieved June 23, 2024, from https://www.tcsg.edu/about-tcsg/system-office-services/data-research/enrollment-graduates/

Enterprise Artificial Intelligence Responsible Use. (2023, October 5). https://gta-psg.georgia.gov/psg/enterprise-artificial-intelligence-responsible-use-ps-23-001

Fair, L. (2022, November 15). *Compliance deadline for certain revised FTC Safeguards Rule provisions extended to June 2023*. Federal Trade Commission. https://www.ftc.gov/business-guidance/blog/2022/11/compliance-deadline-certain-revised-ftc-safeguards-rule-provisions-extended-june-2023

Family Educational Rights and Privacy Act: Guidance for School Officials on Student Health Records | Protecting Student Privacy. (2023, April). https://studentprivacy.ed.gov/resources/family-educational-rights-and-privacy-act-guidance-school-officials-student-health

Governor's Budget Reports | Governor's Office of Planning and Budget. (n.d.). Retrieved June 23, 2024, from https://opb.georgia.gov/budget-information/budget-documents/governors-budget-reports

Grajek, S. (2022). The 2022 Top 10 IT Issues: The Higher Education We Deserve. *Change*, *54*(6), 33–39. https://doi.org/10.1080/00091383.2022.2128022

Grama, J. L. (2020). *Legal issues in information security*. Jones & Bartlett Learning.

Kaczorowska-Spychalska, D., Mazurek, G., Kotula, N., & Sułkowski, Ł. (2024). GENERATIVE AI AS SOURCE OF CHANGE OF KNOWLEDGE MANAGEMENT PARADIGM. *Human Technology*, *20*(1), 131–154. https://doi.org/10.14254/1795-6889.2024.20-1.7

Kam, H.-J., Kim, D. J., & He, W. (2022). Should we wear a velvet glove to enforce Information security policies in higher education? *Behaviour & Information Technology*, *41*(10), 2245–2259. https://doi.org/10.1080/0144929X.2021.1917659

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*, *37*(3), 758–787. https://doi.org/10.1080/07421222.2020.1790190

Mahfuri, M., Ghwanmeh, S., Almajed, R., Alhasan, W., Salahat, M., Lee, J. H., & Ghazal, T. M. (2024). Transforming Cybersecurity in the Digital Era: The Power of AI. *2024 2nd International Conference on Cyber Resilience (ICCR)*, 1–8. https://doi.org/10.1109/ICCR61006.2024.10533072

McIntosh, A. (2022, May 3). *How to Ensure FERPA Compliance in Colleges and Universities*. Technology Solutions That Drive Education. https://edtechmagazine.com/higher/article/2022/05/how-ensure-ferpa-compliance-colleges-and-universities-perfcon

Moustakas, C. E. (1994). *Phenomenological research methods*. Sage.

NexusAI - AI Machine Learning & Cybersecurity | Proofpoint US. (2021, May 11). Proofpoint. https://www.proofpoint.com/us/solutions/nexusai

Patel, J., Manetti, M., Mendelsohn, M., Mills, S., Felden, F., Littig, L., & Rocha, M. (2021, March 24). *AI Brings Science to the Art of Policymaking*. BCG Global. https://www.bcg.com/publications/2021/how-artificial-intelligence-can-shape-policy-making

Raimundo, R., & Rosário, A. (2021). The Impact of Artificial Intelligence on Data System Security: A Literature Review. *Sensors*, *21*(21), Article 21. https://doi.org/10.3390/s21217029

Ryzheva, N., Nefodov, D., Romanyuk, S., Marynchenko, H., & Kudla, M. (2024). Artificial Intelligence in higher education: Opportunities and challenges. *Amazonia Investiga*, *13*(73), 284–296. https://doi.org/10.34069/AI/2024.73.01.24

Sander, C. (2023, May 10). *After a Cyber Attack: Dos and Don'ts for Higher Education IT Staff -*. Campus Technology. https://campustechnology.com/articles/2023/05/10/after-a-cyber-attack-dos-and-donts-for-higher-education-it-staff.aspx

Securing a global solutions landscape. (2024, April 25). https://www.ibm.com/case-studies/sutherland

Terrell, S. R. (2016). *Writing a proposal for your dissertation: Guidelines and examples*. The Guilford Press.

The CrowdStrike Falcon® platform. (n.d.). Crowdstrike.Com. Retrieved June 23, 2024, from https://www.crowdstrike.com/platform/

The Gramm-Leach-Bliley Act (GLBA). (n.d.). Retrieved April 21, 2024, from https://www.stjohns.edu/office-information-technology/technology-labs-and-resources/information-security-and-compliance/gramm-leach-bliley-act-glba

The Snowflake AI Data Cloud. (n.d.). Retrieved February 9, 2025, from https://www.snowflake.com/content/snowflake-site/global/en

UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion. (2024, June). Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

University System of Georgia Enrollment Hits Record High of 344,392 | Communications | University System of Georgia. (n.d.). Retrieved June 23, 2024, from https://www.usg.edu/news/release/university_system_of_georgia_enrollment_hits_record_high_of_344392

Watkins, O. (2024, April 19). *4 use cases for AI in cyber security* [Corporate Blog]. https://www.redhat.com/en/blog/4-use-cases-ai-cyber-security

Whalley, C., Kenslea, M., Ramachandra, A., & Fletcher, S. (2024, January 25). *Cybersecurity Incident Management and Response Guide*. EDUCAUSE Review. https://er.educause.edu/articles/2024/1/cybersecurity-incident-management-and-response-guide

Wirjo, A., Calizo, S., Vasquez, G. N., & San Andres, E. A. (2022). Artificial Intelligence in Economic Policymaking. *The APEC Policy Support Unit*, *222-SE-01.18*(POLICY BRIEF No. 52). https://www.apec.org/docs/default-source/publications/2022/11/artificial-intelligence-in-economic-policymaking/222_psu_artificial-intelligence-in-economic-policymaking.pdf