Portfolio Project

EDUC 765: Trends and Issues in Instructional Design

By: Katie Busch

Submitted June 18, 2025

Project Title: Cybersecurity risks posed by AI systems

Sponsoring Organization

Stratoview Analytics is a mid-sized marketing firm founded in 2018. The company helps clients in industries like finance, healthcare, and retail improve their branding, advertising, and customer outreach using data-driven strategies and digital tools.

Project Description

Stratoview Analytics currently lacks formal AI-use protocols and employee training. In the past year, multiple Stratoview employees have used private generative AI tools like ChatGPT and Google Gemini to assist with workflow. Sometimes these employees uploaded client data and other potentially sensitive information to the AI systems, which presents a significant risk for the firm. Stratoview has not yet implemented a companywide approach to generative AI, and this lack of clarity adds to the cybersecurity risks. However, the firm recently adopted Microsoft Copilot for Microsoft 365 as the companywide approved AI program, as outlined in a contractual agreement. The opportunities for training include the following:

- Ensured protection of sensitive client data
- Better knowledge of cybersecurity risks posed by AI
- Proficient use of Microsoft Copilot for Microsoft 365 within professional workflows
- Adoption and implementation of strategic companywide AI policy

Aim

Protect the firm from employee-generated cybersecurity risks posed by the current usage of generative AI in the workplace. Increase awareness of cybersecurity risks and adopt a strategic protocol for the use of AI through Microsoft Copilot for Microsoft 365. Inform employees of companywide AI policies and acceptable use guidelines.

Target Audience

The primary audience is composed of 60 employees in the areas of: analysts, project managers and marketing specialists. Most have a bachelor’s or master’s degree and have had mandatory training in the past regarding 2-factor authentication and phishing scams, but few have had

formal cybersecurity training. Mandatory training in the past also did not collect specific data related to cybersecurity or generative AI.

Delivery Options

The instructional content will be delivered in a blended learning model, with some learning happening in-person and some asynchronously through learning modules. In-person learning will roll out the companywide AI policy and usage guidelines for Microsoft Copilot for Microsoft 365. Core learning will occur through interactive models consisting of: video lessons, scenario-based problems and checks for understanding.

Instructional Need

Stratoview Analytics is a fictional company created for the purposes of this instructional design project. To ground the project in credible, real-world data, findings from the 2024 Verizon Data Breach Investigations Report (DBIR) are used to inform the instructional need and proposed solution. The DBIR provides industry-wide insights into cybersecurity threats, including employee use of generative AI tools, which closely align with the risks identified in this scenario.

According to the Verizon 2024 Data Breach Investigation Report (DBIR), “A closer-to-home emerging threat from AI is the potential for corporate-sensitive data leakage to the GenAI platforms themselves, as 15% of employees were routinely accessing GenAI systems on their corporate devices (at least once every 15 days). Even more concerning, a large number of those were either using non-corporate emails as the identifiers of their accounts (72%) or were using their corporate emails without integrated authentication systems in place (17%), most likely suggesting use outside of corporate policy.” This presents a significant risk because this sensitive data being shared by employees can be stored on third party servers, accessible to the AI company, or potentially leaked. This may violate privacy laws and contractual agreements outlining the firm’s promise to protect client data.

There is a critical need for employee training regarding these risks, as most employees believe this use of AI is ‘harmless’ and don’t fully comprehend the potential for leaks. Furthermore, there is a clear anticipated need to implement a companywide policy regarding the use of AI. The firm will be implementing a new companywide paid plan with Microsoft Copilot for Microsoft 365. Use of this system is in accordance with contractual agreements that ensure employee data is not stored or used for model training. Additionally, the contractual agreement ensures that all AI interactions are governed by strict data security and compliance protocols. The instructional intervention will train employees on this approved AI system while educating them on the risks of using non-approved consumer-grade tools like ChatGPT or Google Gemini on their employee issued technology or for any work-related tasks.

Learner Analysis

Primary Audience

- Data analysts who frequently work with client data and reports.
- Project managers coordinating client deliverables.
- Marketing specialists using generative AI to support content creation for clients.

Secondary Audience

- IT support staff, specifically those involved in software integration.
- New hires undergoing onboarding and employee training.
- Senior leadership interested in risk management and cybersecurity.

General Learner Characteristics

- Ages 25-54, majority hold a bachelor's or master's degree. Most degrees are in business, data science, marketing or computer science. Ages are not specifically relevant but younger employees may generally be more familiar with AI, particularly from use in educational contexts.
- Most employees earn a salary of between 95,000 – 130,000 yearly. This places most in the upper middle class in MN.
- All employees conduct business in English but some are bilingual (7%). Most common additional languages are: Hindi, Telugu and Spanish.
- 42% of employees in the company self-identify as racial/ethnic minorities. 8% of employees self-identify as LGBTQ+. This will be important when considering diverse perspectives in the learning.
- Around 4% of employees self-identify as having a disability. This is important to consider when creating accessible content and instruction.
- Primarily hybrid or remote workers using company-issued Windows laptops. All employees have access to Microsoft 365, Zoom, and Viva Learning access. This is relevant for technology delivery methods in training and insuring platform consistency.
- Mixed technical literacy, some early adopters of generative AI. Relevant to design differentiated content based on experience with AI.

- Employees are located throughout the United States, but are expected to be able to travel to Minneapolis for meetings at least twice a quarter. Employees' geographic location or timezone is relevant when coordinating meetings.

Entry Characteristics

- Proficiency in Microsoft 365, notably Teams, Outlook, and Excel
- Proficiency and experience leading virtual meetings through Zoom
- General openness to new technology, but limited understanding of how AI systems store data and use data to train new models
- Some employees already have knowledge of AI tools like ChatGPT.
- Exact familiarity with non-training-related software is irrelevant.

Contextual Analysis

Orienting Context

- Learners have expressed in informal conversations and internal feedback sessions that they regularly use generative AI tools like ChatGPT or Gemini to support work tasks, but are unsure of company policies regarding their use.
- High perceived utility of the course, as indicated by the survey data. Employees are eager to learn about AI in the workplace.
- Learners' perceptions of accountability is high as they see AI as highly useful but still a but unregulated in the workplace.
- Common misconceptions indicate learners consider AI use to be 'harmless'; there is limited understanding of the cybersecurity risks. For example, as indicated in the Verizon 2024 DBIR, 15% of employees were routinely accessing generative AI systems on their corporate devices (at least once every 15 days).

Instructional Context

- 8-10 AM Thursdays during regular team meetings, remote/work from home work is done via Zoom, in-person meetings are in Conference Room 2A
- Lighting is standard overhead conference room
- Noise is limited with doors closed
- Temperature 71 degrees Fahrenheit
- Seating is at a large conference table, includes seating for 40 individuals

- AI summaries included in all Zoom meetings, recordings of meetings can be made available internally
- All employees are issued company Windows laptops with company Zoom logins. There is no time limit.
- Employees drive to the North Loop in Minneapolis headquarters for in-person meetings, or join from their home office when working remote.

Technology Inventory

- Learners have access to Office 365 products, Zoom, and the internal learning software Microsoft Viva Learning (part of Microsoft 365 system).
- Employees will have access to the Enterprise Plan - Microsoft Copilot for Microsoft 365 as the company approved avenue for AI use in the workplace.

Transfer Context

- Learning is expected to be highly transferable outside of the company context as generative AI becomes more frequent in daily life. Instruction must connect specifically to real-life scenarios to ensure high learner motivation.
- Expected opportunities for employees to educate their own social networks about the potential dangers of sharing sensitive information with AI programs, specifically those who have school aged children.
- Learning is expected to be perceived as highly relevant to all industries. Tasks must be intermediate in difficulty to encourage motivation

Application of Learning Theories

In line with recommendations from Knowles, Holton, and Swanson (2005), the training program will incorporate best practices for adult learners. Instruction will be guided by Knowles' theory of andragogy, which emphasizes that adult learners are self-directed, bring a wealth of experience to the learning environment, are goal-oriented, and require relevance and immediate application of their learning in the real world.

The program will clearly articulate learning objectives and how each module benefits participants in their professional roles, which addresses the principle of readiness to learn. Learning experiences will be problem-centered based on the adult preference for practical, real-world applications. For example, case studies and simulations related to AI decision-making in their own workplace will be used.

To support self-direction, learners will have opportunities to co-construct goals and reflect on progress. They will be asked to draw from their own experiences and prior knowledge of AI systems. Frequent self-assessment tools will allow learners to monitor their understanding and adjust their approach as needed.

The training design also incorporates Backward Design principles (Wiggins & McTighe, 2005). Learning begins with clearly defined outcomes and assessments so adults know exactly what is expected and what will happen in the learning. Time will be used efficiently, and in-person workshops will include regular breaks after the completion of cognitively demanding tasks. Instructors will be fully prepared. If administrated successfully, the learning climate will feel like mutual respect and collaboration.

Elements of Cognitive Load Theory (Sweller, 1988) are reflected in the organization of material to reduce extraneous load. Complex content is chunked into digestible parts, and scaffolding includes supportive visuals and multiple examples.

Some elements of behavioral theory will apply to the self-guided modules. Early interactions will include immediate feedback such as a green check mark and the word "Correct" to reinforce successful learning. The self-guided modules will also feature a human-like AI model to guide participants, which draws from Bandura's Social Learning Theory. The human-like model will demonstrate effective behavior, language, and decision-making strategies in realistic scenarios.

Learners will also be encouraged to expand their learning through personal learning networks, a concept rooted in connectivism. The conversation around AI is expected to continue through social media, news coverage, and workplace discussion.

Application of Motivational Theories

Learning references Keller's instructional model of ARCS. Since motivating learners in e-learning can be more challenging than in-person learning, the factors of Attention, Relevance, Confidence and Satisfaction will be included in the self-guided modules. The element of Attention is already relevant because of the documented interest in AI, but this will be furthered when learners explore the potential risks of data breaches. Specifically, this will draw from the strategy of 'Incongruity and Conflict'. The importance of Relevance cannot be overstated, as AI systems grow more powerful every day. Learning must be useful and relatable to learners' daily lives. The element of Confidence will develop success expectation among learners as they control their learning experiences. Finally, learners should be satisfied with their achievements through the learning process.

Because of the identified interest in generative AI, learners are expected to be highly motivated to explore AI in the workplace. Training must capitalize on this existing interest and encourage learners to fully explore their current use of AI, specifically how they may have contributed to cybersecurity risks unknowingly in the past. Training should be informed by Cognitive Dissonance Theory (Festinger 1957). Employees may realize that actions they thought were benign, such as using AI with personal accounts for workplace projects, may have actually contributed to security breaches. Learners must be made explicitly aware of the risks of inappropriate AI usage and the urgency and importance of the topic.

Impact of a Diverse Audience on Instruction

Stratoview Analytics is committed to DEI programming and actively promotes a culture of inclusion and diverse perspectives in the workplace. According to data provide by Human Resources, 42% of employees in the company self-identify as racial/ethnic minorities and 8% of employees self-identify as LGBTQ+. The instructional leadership team must ensure learning activities are culturally responsive, accessible and relevant. This includes using inclusive language, representing diverse perspectives and scenarios in training materials, and proactively addressing potential barriers to engagement or comprehension. Instructional leadership should consult with Subject Matter Experts, including those with lived experience related to the training

content, for feedback. Feedback should be solicited from Employee Resource Groups (ERGs) or DEI liaisons to identify blind spots ensure cultural relevance in the learning.

Goal Analysis

Instructional Goal

Learners will be able to confidently and ethically use Microsoft Copilot, the company-approved AI tool, in the workplace. They will demonstrate knowledge of key concepts including: AI, prompt generation, data storage, cybersecurity, and ethical decision making. Learners will be able to explain the risks associated with using unapproved AI tools and provide concrete examples of misuse. They will also articulate the importance of a strict company AI policy to mitigate potential risks. Finally, learners will develop a personal opinion regarding the productive and responsible use of AI and apply Copilot effectively to enhance productivity in their specific role.

Task Analysis Method

Topical analysis – I chose this method because it seemed the most straightforward for my goals. This project contains multiple procedures, definitions, and ultimately learners form their own opinions on AI systems, so I thought topical would fit all of those types of learning best.

Task Analysis

Conduct task analysis here:

Part 1: Identify Content Structures:

Facts:

-Develop a basic working definition of the terms: ‘generative AI’, ‘Artificial Intelligence’, ‘prompt’ etc.

-Define ‘cybersecurity risk’

Concepts:

-concept of cybersecurity
-concept of risk
-concept of generative AI
-concept of data privacy

Principles and Rules:

-How personal AI systems (ChatGPT, Gemini) store user data and train future AI models vs. how Copilot (paid, companywide AI system) does not do this
-How sharing data with these systems poses a cybersecurity risk
-How prompts affect answers from AI

Procedures:

-How to access / open Copilot on employee laptop through work email account
-How to contact tech for help
-How to form an effective prompt for Copilot
-How to inform tech if they encounter a potential cybersecurity risk
-How to differentiate between helpful vs. unhelpful responses and use prompts to get closer to desired response
-How to identify helpful vs. unhelpful contexts for using AI in the workplace
-How to deactivate personal AI systems on work computers

Attitudes:

-Misuse of client data
-Appropriate use of AI systems
-Cybersecurity risks as preventable

Part 2: Group Related Content Structures:

Introduction

-Develop a basic working definition of the terms: ‘generative AI’, ‘Artificial Intelligence’, ‘prompt’ etc. (fact)

-concept of generative AI (concept)

How to Use AI

-How to identify helpful vs. unhelpful contexts for using AI in the workplace (Procedures)

-Appropriate use of AI systems (Attitudes)

-How to access / open Copilot on employee laptop through work email account (Procedures)

-How to contact tech for help (Procedures)

-How to inform tech if they encounter a potential cybersecurity risk (Procedures)

-How to deactivate personal AI systems on work computers (Procedures)

Prompts

-How to form an effective prompt for Copilot (Procedures)

-How prompts affect answers from AI (Principles and Rules)

-How to differentiate between helpful vs. unhelpful responses and use prompts to get closer to desired response (Procedures)

Cybersecurity Risks

-Define ‘cybersecurity risk’ (fact)

-concept of cybersecurity (concept)

-concept of risk (concept)

-Cybersecurity risks as preventable (Attitudes)

Data

-concept of data privacy (concept)

-How personal AI systems (ChatGPT, Gemini) store user data and train future AI models vs. how Copilot (paid, companywide AI system) does not do this (Principles and Rules)

-How sharing data with these systems poses a cybersecurity risk (Principles and Rules)

-Misuse of client data (Attitudes)

Part 3: Detailed Outline

Introduction

AI

1. AI (Artificial Intelligence)
    a. the ability of machines or software to perform tasks that typically require human intelligence
        i. such as understanding language
        ii. recognizing patterns
        iii. solving problems
        iv. making decisions.
    b. Types of AI

        i. Chat GPT
        ii. Gemini
        iii. Copilot
2. Generative AI
    a. a type of artificial intelligence that can create new content based on the data it was trained on
    b. Uses patterns and massive amounts of data to create original content
    c. Adapts and responds based on user input
        i. Based on your activity, will be different for each person
            1. Consider how social media algorithms make content unique for each person
        ii. AI doesn't necessarily always have the **best/right** answers, it will give you the answer it thinks you want to see based on past interactions
3. Prompt
    a. the input that a user gives to an AI system to get a response
    b. usually a question or instruction
        i. Sentence frames for prompts:
            1. How can I
            2. Where can I find
            3. Create a
        ii. Examples – write an email for my boss…

How to Use AI

How to identify helpful vs. unhelpful contexts for using AI in the workplace (Procedures)

1. Helpful uses
    a. Generating emails (but user edits after)
    b. Scheduling
    c. Checking 'tone' of speech (especially if communicating in non-native language)
2. Unhelpful uses

    a. Generating emails (but user edits after)
        i. Can be obvious when someone uses AI
            1. Lots of dashes
            2. Long sentences: verb + ing + comma
            3. Does this actually sound like __?
    b. Plagiarism
    c. Connect to learners' prior experiences
        i. What has been helpful / unhelpful?
        ii. Add to list
    d. Bias from incomplete data
    e. AI influencing human decision making
        i. Recommendation algorithms
            1. Youtube (ex: watch next recommended video)
    f. Reduction in critical thinking
3. How to identify helpful vs unhelpful

How to access / open Copilot

1. Log in to employee laptop
2. Open preferred browser
3. Navigate to Microsoft 365
    a. www.office.com
4. Sign in using work email and password
5. Look for Copilot icon or select a supported app
    a. Word
    b. Excel
    c. Outlook
6. Click on the Copilot feature
    a. Often on sidebar
    b. Might be labelled 'AI assistant'
7. Begin interacting with Copilot
    a. Prompt generation

How to contact tech for help

1. Submit a help ticket or send an email
2. Call the IT support line
3. Include Key information

How to inform tech if they encounter a potential cybersecurity risk

1. Respond immediately
2. Submit a help ticket or email tech
3. Do not interact further with the suspicious file, link, AI system, etc.
4. Include specifics
    a. Screenshots

How to deactivate personal AI systems on work computers (Procedures)

1. Open the Application or extensions settings on your device
2. Identify the AI tools you're logged into
3. Uninstall or disable them
4. Notify IT that personal AI tools have been removed as per compliance

Prompts

1. How to form an effective prompt for Copilot (Procedures)
    a. Clear and direct statements or questions
    b. Include context
        i. Ex: who is the email for?
        ii. Ex: explain x for someone with no technical background
    c. State desired format
        i. Bullet points

        ii. Table
        iii. Statement
    d. Role-based prompts
        i. Ex: pretend you are an IT trainer. Write a script to …
2. How prompts affect answers from AI (Principles and Rules)
    a. Clarity leads to more accurate responses
3. How to prompts to get closer to desired response (Procedures)
    a. Add more context
    b. Be specific
    c. Ask follow up questions

Cybersecurity Risks

1. Define ‘cybersecurity’
    a. the practice of protecting systems, networks, and data from digital attacks, unauthorized access, damage, or theft
2. Define ‘cybersecurity risk’
    a. potential for loss, damage, or harm resulting from a failure to protect digital systems
3. Describe cybersecurity risks as preventable
    a. Daily choices and data usage
    b. Shift thinking from risks being ‘beyond my control’
        i. Use company approved software and data protection tools
        ii. Preventable by using pre-approved AI systems (Copilot)

Data

1. Concept of data privacy
    a. Right of individuals or companies to control how their personal or sensitive information is stored and used
        i. Examples in the workplace: client data, employee records, financial data
    b. Respecting confidentiality

How public AI systems (ChatGPT, Gemini) store and use data

1. Collect and store data
2. Data may be used to train future models
    a. What you type may be used to teach new AI systems and could appear in someone else's response
3. Creates preventable cybersecurity risk

How Copilot (paid, companywide AI system) uses data

1. Enterprise use (paid model)
    a. the company's data privacy agreements apply (not the AI platform's)
    b. does not use your inputs to train any AI models
    c. data remains secure within the company's cloud

Terminal Objectives and Enabling Objectives

Terminal Objective: Learners will be able to effectively use company-approved Microsoft Copilot (AI system) to complete work-related tasks. (cognitive, affective)

Enabling Objectives:

- Access and open Copilot on company device. (psychomotor)
- Generate clear and precise AI prompts. (cognitive)
- Identify appropriate vs. inappropriate uses of AI in the workplace. (cognitive)
- Demonstrate responsible, ethical use of AI systems. (affective, cognitive)

Terminal Objective: Learners will be able to explain the risks involved when using unapproved AI systems in the workplace. Additionally, learners will be able to describe how Copilot mitigates common cybersecurity risks. (Cognitive)

Enabling Objectives:

- Define key terminology: cybersecurity risk, generative AI, prompt (Cognitive)
- Describe how unapproved AI systems (like ChatGPT and Gemini) store and potentially reuse user data (Cognitive)
- Explain how the company approved AI system (Copilot) does not store data. (Cognitive)
- Identify examples of sensitive data that should not be shared with personal AI. (Cognitive)
- Report potential security breaches appropriately and in line with company policy. (Cognitive)

Terminal Objective: Learners will be able to demonstrate appropriate and ethical use of AI systems in the workplace.

Enabling Objectives:

- Develop and describe a personal opinion of ethical AI usage. (Affective)
- Avoid potential cybersecurity risks by only using company approved AI software (Copilot). (Cognitive)

[redacted]

Title of the unit/module: Cybersecurity Risks Posed by AI Systems

Brief description of target audience: 60 employees at Stratoview Analytics, a midsized marketing firm in Minneapolis, MN. Most hold bachelor's or master's degrees and have varying levels of understanding of AI systems, data privacy, and cybersecurity. They've completed basic IT training but have not had formal education on AI. The team works on company-issued laptops through Microsoft 365. They will be learning the companywide policy regarding Copilot as the official workplace AI system of choice and the risks involved with using unapproved AI systems in the workplace.

List Terminal Objective Here: Learners will be able to explain the risks involved when using unapproved AI systems in the workplace. Additionally, learners will be able to describe how Copilot mitigates common cybersecurity risks. (Cognitive)

List Pre-Instructional Strategy: pretest

Enabling Objective	Level on Bloom's Taxonomy	Learner Activity (What would learners do to master this objective?)	Delivery Method (Group presentation/lecture, self-paced, or small group)
Define key terminology: cybersecurity risk,	Remembering	Complete a short-answer quiz	Self-paced

Enabling Objective	Level on Bloom's Taxonomy	Learner Activity (What would learners do to master this objective?)	Delivery Method (Group presentation/lecture, self-paced, or small group)
generative AI, prompt (Cognitive)		defining each term in their own words	
Describe how unapproved AI systems (like ChatGPT and Gemini) store and potentially reuse user data (Cognitive)	Understanding	Watch a video / read an article and summarize the risks in a discussion or in on online discussion board	Small group work, share with larger group
Explain how the company approved AI system (Copilot) does not store data. (Cognitive)	Understanding	Explain in their own words how the company-wide paid Copilot AI program differs from free, non-approved AI systems.	Self-paced
Identify examples of sensitive data that should not be shared with personal AI. (Cognitive)	Applying	Create an example of a potential misuse of AI that could happen in the workplace and explain why it is harmful.	Small group work, share with larger group
Report potential security breaches appropriately and in line with company policy. (Cognitive)	Applying	Complete the company-approved process for reporting potential security breaches.	Self-paced

Keller, J. M. (2010). *ARCS model of motivational design* [Handout]. Texas A&M University System. https://www.tamus.edu/academic/wp-content/uploads/sites/24/2017/07/ARCS-Handout-v1.0.pdf

Knowles, M., Holton, E. F., & Swanson, R. A. (2005). *The adult learner: The definitive classic in adult education and human resource development* (6th ed.). Elsevier.

Mager, R. F. (1997). *Preparing instructional objectives: A critical tool in the development of effective instruction* (3rd ed.). Center for Effective Performance.

Malamed, C. (n.d.). *Motivation in instructional design*. The eLearning Coach. https://www.instructionaldesign.org/concepts/motivation/

Sweller, J., van Merriënboer, J. J. G., & Paas, F. G. W. C. (1998). Cognitive architecture and instructional design. *Educational Psychology Review, 10*(3), 251–296. https://doi.org/10.1207/s15516709cog1202_4

Wiggins, G., & McTighe, J. (2005). *Understanding by design* (2nd ed.). Association for Supervision and Curriculum Development.