Needs Analysis: Cybersecurity Compliance Training

Data Privacy & Remote Work Security Awareness

An instructional design needs analysis conducted during the Analysis phase of ADDIE, applying adult learning principles, accessibility standards, and stakeholder input. This portfolio case study showcases a comprehensive approach to developing effective cybersecurity training for today's distributed workforce.

Purpose of Training

Addressing Emerging Risks

Remote and hybrid work environments create significant risks for data breaches, phishing attacks, and compliance violations. The distributed nature of today's workforce requires specialized awareness training.

This training ensures employees, contractors, and retirees understand organizational cybersecurity standards, privacy responsibilities, and secure practices regardless of work location. By addressing specific threats in remote environments, we can maintain data integrity while supporting flexible work arrangements.

Target Audience & Accessibility

Dummy Data

Active Employees

- Ages 23-65, diverse technical abilities
- Working on company laptops and personal devices
- 5% require screen readers or keyboard navigation
- 10% are non-native English speakers
- Primary concerns: Quick completion, practical application

Retired Associates

- Ages 62-80, varied digital literacy
- Accessing via personal computers and tablets
- 15% require larger text and high contrast
- 8% use assistive technologies
- Primary concerns: Clear instructions, technical support

Accessibility Considerations

All training materials must adhere to WCAG 2.1 standards, including proper contrast ratios, keyboard navigation, alternative text, and compatibility with screen readers. Universal Design for Learning principles ensure multiple means of engagement, representation, and action/expression.

Organizational Needs & Gaps

Dummy Data

Current State

- 43% of employees use weak or duplicate passwords
- 27% increase in phishing incidents since remote work began
- 19 compliance violations in the past quarter
- 68% of employees share sensitive files via email
- Only 35% of retirees use two-factor authentication

Desired State

- 100% strong password compliance
- 90% phishing email identification accuracy
- Zero compliance violations
- Secure file-sharing practices across all departments
- Universal adoption of two-factor authentication

The gap analysis reveals critical vulnerabilities in our remote work security posture that must be addressed through targeted training interventions.

Stakeholder Input

> "Our biggest vulnerability isn't our systems - it's our people. We need training that creates security awareness as second nature, especially for those working from home without the protective infrastructure of our offices."

Jane Doe, IT Security Officer

> "Compliance isn't just about checking boxes. We need our people to understand why these protocols exist and how they protect both our clients and our organization from potential breaches."

Wesley Johnson, HR Compliance Manager

> "Many retirees maintain access to sensitive company information but often feel overwhelmed by rapidly changing security requirements. We need clear, straightforward guidance without technical jargon."

Faye Stevenson, Retiree Cohort Representative

Stakeholder interviews revealed consistent themes around simplicity, practical application, and making security awareness intuitive rather than burdensome. These insights directly informed our learning objectives and instructional approach.

Learning Objectives Matrix

Identify Phishing Attempts (Analyze)

Instructional Approach: Inbox simulation with clickable hotspots highlighting suspicious sender, links, and attachments (Mayer: signaling & contiguity; Merrill: problem-centered).

Assessment: Scenario-based activity: Learner clicks elements of a suspicious email → receives immediate feedback on accuracy.

Secure File Sharing (Apply)

Instructional Approach: Demonstration of insecure vs. secure file sharing (e.g., emailing vs. cloud system). Integration of case studies (Merrill: demonstration → application).

Potential Future Dev - Assessment: Branching scenario: “Share a file with a colleague securely” (choose the correct method). Score/feedback given.

Handle Two-Factor Authentication (Apply)

Instructional Approach: Guided walkthrough of authentication process with screen capture demo (Gagné: provide guidance, elicit performance).

Assessment: MCQ; future dev - Simulation: Learner completes mock 2FA steps (receives success/failure feedback).

Respond to Security Threats (Evaluate)

Instructional Approach: Scenario-based branching narrative: paths showing poor vs. compliant decisions (Merrill: problem → apply).

Potential Future Dev - Assessment: Role-play simulation with escalating security incidents (90% protocol adherence)

Each objective directly addresses identified organizational gaps while incorporating stakeholder priorities for practical application and real-world relevance.

Design Principles Applied

Bloom's Taxonomy

Objectives span multiple cognitive levels (Remember through Evaluate) to ensure both foundational knowledge and higher-order application. This supports transfer to authentic contexts.

Merrill's Principles

Training activates prior knowledge, demonstrates skills, provides application opportunities, and integrates into real-world workplace scenarios, following problem-centered design.

Gagné's Nine Events

Structured learning experience with attention-grabbing scenarios, clear objectives, scaffolded instruction, guided practice, and transfer support to real-world situations.

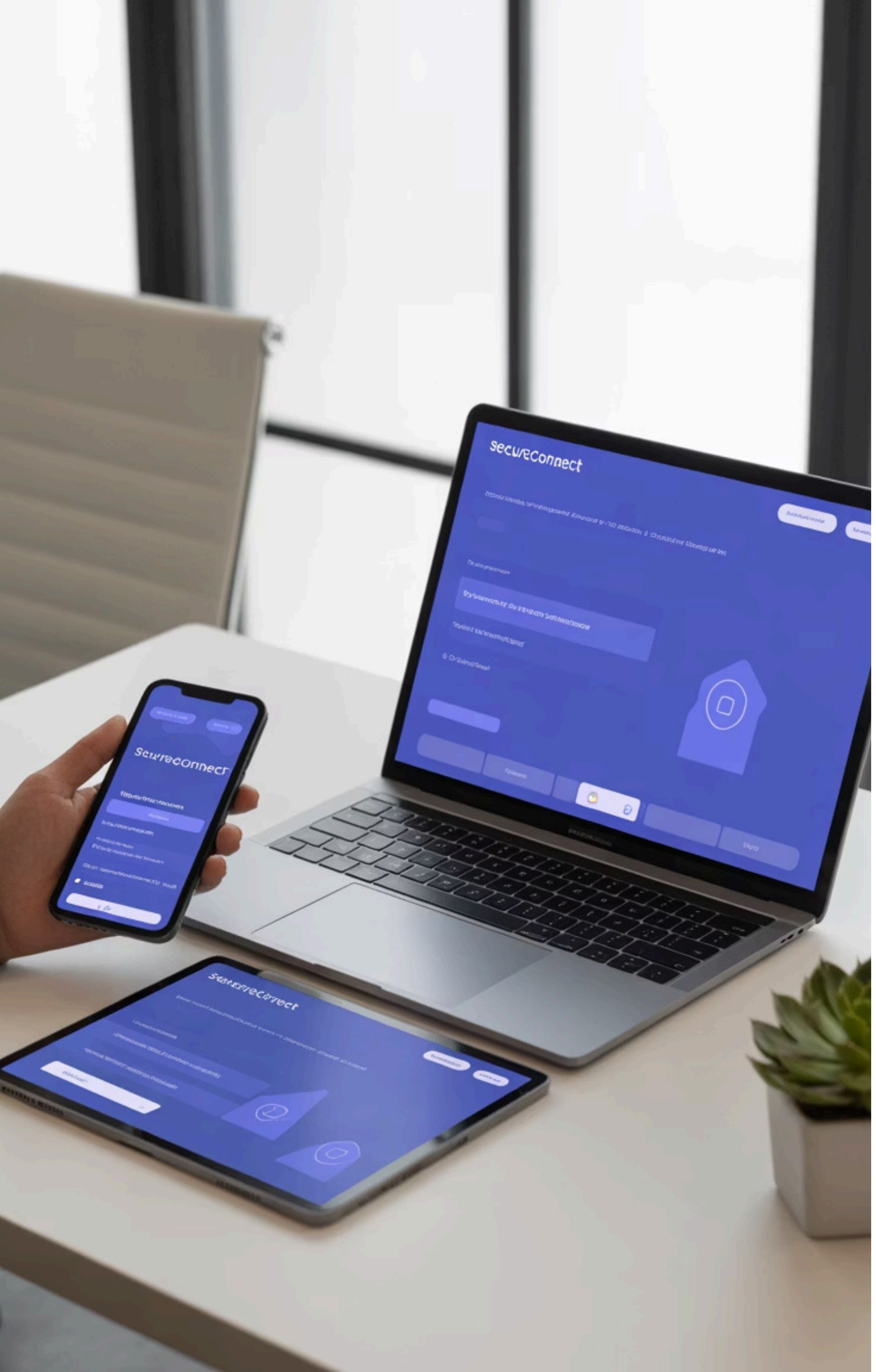
Mayer's Multimedia Principles

Applied contiguity, modality, and coherence principles to reduce cognitive load and maximize retention. Audio narration pairs with visuals, extraneous content is eliminated.

UDL/WCAG Accessibility

Multiple representation methods (text, audio, visual), engagement approaches, and expression options ensure equitable access for all learners regardless of ability.

These frameworks guided all instructional decisions, ensuring an evidence-based approach to cybersecurity training that balances learning science with practical workplace needs.



Potential Training Modalities

Microlearning Modules

2-4 minute focused lessons on specific security skills, accessible on any device for just-in-time learning

Virtual Workshops

Monthly 30-minute facilitated sessions for practice, questions, and peer learning opportunities

Interactive Simulations

Realistic security scenarios requiring decision-making and application of protocols under pressure

Blended Approach Rationale

The mixed-modality approach addresses varied learning preferences, technical comfort levels, and accessibility needs while providing both structured instruction and on-demand reinforcement. All components are mobile-responsive with offline capabilities for field employees.

Data Collection & Measurement

Dummy Data

83%

Knowledge Retention

Target retention rate measured through periodic knowledge checks at 30, 60, and 90 days post-training

90%

Phishing Detection

Success rate in identifying test phishing emails sent by IT security team monthly

35%

Incident Reduction

Target decrease in security incidents and compliance violations within six months of training implementation

Learning Analytics

- Completion rates by demographic
- Time spent on learning activities
- Common mistake patterns
- Engagement metrics by content type

Business Impact Metrics

- Help desk tickets related to security
- Compliance audit scores
- Data breach prevention ROI
- Recovery time for security events

Comprehensive data collection allows for continuous improvement while demonstrating training ROI to stakeholders. All metrics tie directly to identified organizational gaps and business objectives.

Next Steps in ADDIE Process

1

Analysis

✓ COMPLETED

- Needs assessment
- Audience analysis
- Gap identification
- Stakeholder interviews

2

Design

NEXT PHASE

- Storyboard development
- Content mapping
- Interaction design
- Assessment strategy

3

Development

UPCOMING

- Content creation
- Media production
- Platform integration
- Accessibility testing

> **This needs analysis has informed the design of targeted, inclusive cybersecurity training that addresses real organizational gaps while accommodating diverse learner needs.**

View Course

View Project Details