2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC
Host Sponsor UNC Charlotte
ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION
Paper ID #51256

CIME: A Scenario-Based Framework for Cyber Preparedness and Strategic Response

Dr. Douglas W. Jacobson, Iowa State University of Science and Technology

Doug Jacobson is a University Professor in the Department of Electrical and Computer Engineering at Iowa State University. He is currently the director of the Iowa State University Center for Cybersecurity Innovation and Outreach, which has been recognized by the National Security Agency as a center of academic excellence. He has worked for years on ways to include cybersecurity in courses and the general population. Doug also created the Iowa Cyber Hub, which is dedicated to increasing the cyber workforce in Iowa. Doug has given over 300 presentations in the area of computer security. He also created the cybersecurity ambassador program targeted at the general public, K-12 students, post-secondary students, and employees.

Jennifer Horn-Frasier

Jennifer Horn-Frasier is a strategy consultant and education leader based in Iowa City, Iowa. Her work focuses on strengthening collaboration between education, industry, and community partners, drawing on experience as a public school teacher, nonprofit leader, and systems-level strategist. As a fellow of the Strategic Doing Institute, she helps organizations and community coalitions move from ideas to coordinated action through the application of Strategic Doing, a framework that guides cross-sector teams in addressing complex challenges and advancing strategy as a learning-oriented, iterative process. She is also an active civic leader and elected director of the Iowa City Community School District Board of Education, with a commitment to championing inclusive, high-quality public education.

©American Society for Engineering Education, 2026

CIME: A Scenario-Based Framework for Cyber Preparedness and Strategic Response

1. Introduction

Cyber incidents rarely remain confined to information technology departments. Disruptions caused by ransomware, data loss, service outages, or business email compromise frequently impact frontline operations, leadership decision-making, public trust, and an organization's ability to deliver essential services [1]. Yet many cybersecurity tabletop exercises and training approaches continue to emphasize technical response and system recovery, implicitly framing cyber incidents as problems to be solved primarily by IT staff.

This technical-centric framing creates a gap in preparedness. Non-IT personnel, including administrators, managers, communicators, and frontline workers, are often critical to sustaining operations during a cyber incident; yet, they frequently lack structured opportunities to practice decision-making, coordination, and communication in disrupted environments. Addressing this gap requires educational approaches that treat cybersecurity incidents as organizational challenges rather than purely technical failures.

This paper presents the Cybersecurity Incident Management Exercises (CIME) framework, a scenario-based educational approach designed to prepare participants to manage the effects of cyber disruptions rather than immediately resolve them. The CIME framework was developed and deployed through applied cybersecurity education and outreach activities at Iowa State University's Center for Cybersecurity Innovation and Outreach. CIME assumes that a breach has already occurred and that technical remediation is not immediately available, shifting attention toward operational continuity, prioritization, and cross-functional coordination. The framework has been deployed across multiple sectors, including local government, medical, transportation, agriculture, and manufacturing, engaging participants with widely varying levels of technical expertise. This work contributes to engineering education by presenting a repeatable, scenario-based framework that develops decision-making, coordination, and socio-technical reasoning skills in both technical and non-technical learners.

Beyond scenario discussion, CIME integrates Strategic Doing [2] as a core pedagogical element. Strategic Doing is a discipline for taking effective action in complex, uncertain situations by bringing diverse stakeholders together to focus on shared outcomes, leverage existing assets, and move forward through short, learning-based action cycles. It reflects how real cyber incidents unfold, requiring clear communication, rapid decision-making, and collective learning when information is incomplete. By embedding Strategic Doing within the exercise structure, CIME emphasizes cybersecurity incident management as a learned and practiced capability rather than a static plan or checklist.

The primary outcomes of the Strategic Doing-powered CIME program to date include: (1) a repeatable, scalable framework for cybersecurity incident management education; (2) a taxonomy to guide exercise design across audiences and role structures; and (3) insights from multi-sector deployments that highlight learning outcomes, facilitation considerations, and

educational implications. The remainder of the paper situates CIME within related work, describes the framework and its pedagogical foundations, presents the exercise taxonomy, and discusses lessons learned and implications for engineering and cybersecurity education.

2. Background and Related Work

Cybersecurity exercises are widely used to prepare organizations for incidents, yet their design and educational focus vary significantly. This section reviews standard exercise models, highlights limitations for non-technical participants, and situates CIME within broader trends in cybersecurity education.

Traditional Cybersecurity Tabletop and Exercise Models

Many cybersecurity tabletop exercises are structured around technical response workflows that emphasize detection, containment, eradication, and recovery. Red team/blue team exercises and incident response drills are valuable for testing technical controls and team readiness, but they often prioritize system-level outcomes over organizational decision-making processes. [3-4] In these formats, non-IT participants may play limited or observational roles, reinforcing the perception that cybersecurity incidents are primarily technical events.

While these approaches are effective for validating technical capabilities, they are less effective in preparing organizations to manage prolonged disruptions, communicate effectively under uncertainty, or coordinate across functional boundaries. As a result, critical non-technical dimensions of cyber incidents, such as service prioritization, public communication, legal considerations, and workforce impacts, may receive limited attention.

Cybersecurity Education Beyond IT

Recent work in cybersecurity education emphasizes the importance of cyber literacy, workforce readiness, and organizational resilience. Scholars and practitioners are increasingly recognizing that effective cybersecurity depends not only on technical expertise but also on diverse stakeholders' ability to understand risks, make informed decisions, and collaborate effectively during incidents. Educational models that engage non-IT participants are therefore essential for developing comprehensive cyber preparedness.

From an educational perspective, cyber incidents present opportunities to teach systems thinking, ethical reasoning, and decision-making under uncertainty. These competencies align closely with engineering education goals, particularly as engineers and technologists are increasingly expected to operate within complex socio-technical systems. [5]

Educational Framing for Incident Management Exercises

Experiential learning, scenario-based instruction, and role-based learning have been shown to support deeper engagement and knowledge transfer in complex domains. By placing participants in realistic, consequence-driven scenarios, these approaches encourage active learning and

reflection. However, without structured mechanisms to guide action and follow-through, scenario-based exercises risk ending with discussion rather than durable learning outcomes.

CIME builds on these educational foundations by combining scenario-based learning with Strategic Doing, creating a structured environment in which participants practice collaboration to prioritize, leverage assets, and plan and execute learning-based action cycles under constraint. This integration distinguishes CIME from traditional tabletop exercises, positioning it as an educational intervention focused on learning rather than mere rehearsal.

3. Methods

This study employs a design-based research approach to examine the development, implementation, and evaluation of the Cybersecurity Incident Management Exercises (CIME) framework across multiple educational contexts. The goal of the study was to assess whether CIME functions as an effective educational intervention for (1) undergraduate students and (2) trained facilitators responsible for delivering the framework in professional and community settings.

Research Design

CIME was implemented and evaluated in two primary contexts during the study period:

1. **Facilitator training program** preparing participants to deliver CIME exercises independently.
2. **Undergraduate classroom pilot (CO-CIME)** involving cybersecurity and business students.

Data were collected using post-intervention surveys consisting of Likert-scale and open-ended items. Analysis focused on descriptive statistics and thematic coding of qualitative responses. This study does not attempt to establish causal impact through controlled experimentation; instead, it provides preliminary evidence regarding perceived educational value and learning outcomes associated with CIME.

Participants

A total of 40 participants completed the structured CIME facilitator training program. Participants represented diverse professional backgrounds, including extension educators, municipal administrators, IT professionals, higher education staff, graduate students, and industry representatives. The training consisted of a five-hour experiential workshop integrating simulation, Strategic Doing instruction, and practice facilitation.

The classroom pilot involved 30 undergraduate students drawn from cybersecurity (technical track) and business (organizational track) programs. Students were organized into mixed-role teams and participated in a four-hour CO-CIME simulation.

Intervention Structure

Both implementations were grounded in the same pedagogical elements:

- Assumed-breach scenario framing
- Five-step incident management process
- Integration of Strategic Doing principles
- Structured facilitation emphasizing equity of voice and asset-based decision-making

The CIME facilitator training included both participation in a CIME mini-simulation and guided practice in facilitating a CIME. The classroom pilot employed a dual-track CO-CIME configuration, integrating CySIM [6] (IT-centric technical track) and CIME (organization-focused track) exercises.

Data Collection Instruments

Post-intervention surveys included:

- 5-point Likert-scale items assessing overall value and preparedness
- Open-ended questions regarding the most valuable aspects of the experience
- Reflection prompts regarding confidence, clarity, and applicability

For the facilitator training, participants assessed the clarity of the framework, their confidence in facilitating, their understanding of Strategic Doing, and their readiness to implement CIME. For the classroom pilot, students rated the overall value of the exercise and provided qualitative reflections.

Data Analysis

Quantitative data were analyzed descriptively (mean, median, frequency distribution). Given the exploratory nature of the study and modest sample sizes, no inferential statistical testing was conducted.

Qualitative responses were reviewed and coded thematically to identify recurring patterns related to:

- Cross-disciplinary collaboration
- Communication under constraint
- Structured decision-making
- Role clarity
- Perceived readiness

Themes were identified through iterative review and consolidation of recurring statements across respondents.

Limitations

This study relies primarily on self-reported perceptions of educational value and preparedness. It does not include pre- or post-measures or longitudinal follow-up, nor does it measure objective performance outcomes. While the findings provide preliminary evidence of the educational utility of CIME, further research is needed to assess its long-term impact, knowledge retention, and behavioral change.

4. The CIME Framework

The Cybersecurity Incident Management Exercises (CIME) framework is designed as an educational intervention that prepares participants to manage cyber incidents as organizational disruptions rather than purely technical failures. The framework intentionally shifts the focus from preventing or immediately resolving a breach to sustaining operations, coordinating across roles, and making informed decisions under conditions of uncertainty.

Design Philosophy

CIME is grounded in several core design principles. First, each exercise assumes that a significant cyber incident has already occurred and that technical remediation is not immediately available. This premise reflects the reality that many real-world incidents involve prolonged disruption, incomplete information, and limited control over affected systems.

Second, CIME separates technical remediation from operational decision-making. While technical context is essential for realism, the exercise is intentionally structured so that non-IT participants must engage directly with the consequences of disruption. This design choice ensures that participants who are responsible for leadership, communication, finance, human resources, and frontline operations actively practice their roles during a cyber incident.

Third, the framework emphasizes communication, prioritization, and adaptation. Rather than optimizing for technically ideal solutions, participants are encouraged to identify what actions are feasible with existing resources and authority. This emphasis mirrors the constraints organizations face during real incidents and reinforces cybersecurity incident management as a socio-technical challenge.

Structure of a CIME Exercise

A CIME event follows a structured yet flexible progression that supports both realism and learning. While the framework can be adapted to different audiences and contexts, the design and execution of exercises typically include the following phases:

Planning. Facilitators work with organizational stakeholders to clarify objectives, understand operational dependencies, and define the scope of the exercise. This phase ensures that simulation scenarios are grounded in the participant environment and aligned with learning goals.

Assessment. Before the exercise, facilitators may collaborate with IT staff to identify critical systems, common failure modes, and plausible threat scenarios. This assessment informs

scenario development while keeping technical details at a level appropriate for non-IT participants. It should be noted that not all CIME exercises need this step.

Exercise Execution. The exercise begins with the presentation of a cyber incident that has already disrupted normal operations. This involves producing a short video tailored to the specific scenario. The video focuses on what is not working (power, phones, computers, etc.) rather than the details of the cyberattack. Examples of the videos can be found on the CIME website [7]. Participants are organized into teams of 6 to 8 engaged. At the same time, one or more trained exercise facilitators guide the groups through the process and ensure that decisions reflect organizational priorities.

Post-Exercise Processing. Immediately following the exercise, participants engage in structured reflection and discussion. This phase focuses on how decisions were made, how information was shared, where assumptions or gaps emerged, and how insights gained from the exercise may be applied in the future.

Post-Event Training and Follow-Up. In many deployments, organizations engage in follow-on activities such as targeted training, planning sessions, or additional exercises. These activities allow participants to practice and internalize the discipline of Strategic Doing, reinforcing learning and supporting sustained improvement.

The Five-Step Incident Management Process

Within the broader exercise structure, CIME uses a five-step incident management process to guide participant discussion and decision-making. This five-step process functions as a cognitive scaffold, guiding participants from sense-making to commitment and reflection.

1. **Problem statement: Where are we now?** Participants establish a shared understanding of the situation, acknowledging uncertainty and incomplete information.
2. **Outcome priorities: What matters most?** Teams create a shared understanding of desired outcomes, based on near-term and medium-term priorities for the organization and its stakeholders.
3. **Asset-based ideation: What could we do?** Participants create a catalog of available assets and brainstorm how these assets may be combined and used to move toward the desired outcomes.
4. **Evaluation of opportunities: What should we do?** Teams evaluate the ease and impact of completing the asset-based actions brainstormed in Step 3.
5. **Iterative action plan: What will we do?** Selecting the options with the greatest potential, as identified in Step 4, teams create action plans with a responsible person clearly assigned to each action. Once the work is started, they meet regularly to share learning, evaluate options, and plan next steps.

Strategic Doing is the framework for this process, guiding participants' decision-making to prioritize actions based on their impact, feasibility, and available resources. This approach encourages teams to move beyond identifying problems toward committing to achievable actions within real organizational constraints.

Execution Flow and Adaptability of CIME Exercises

While all CIME deployments follow a common pedagogical structure, the detailed execution flow varies based on audience, setting, and learning objectives. For example, a "CIME of One" designed for public awareness may emphasize early-stage sense-making and prioritization, while an organizational CIME may allocate more time to action planning and post-exercise reflection.

To support this adaptability, CIME uses a modular run-of-show design that preserves the five-step incident management process while allowing facilitators to adjust timing, regroup points, and depth of discussion. A representative run of show, drawn from deployed CIME exercises, is provided in Appendix A to illustrate how these elements are operationalized in practice.

5. Role of IT in CIME

The role of information technology staff in CIME differs significantly from their role in many traditional cybersecurity exercises. Rather than serving as primary responders responsible for resolving the incident, IT personnel contribute to the exercise in ways that support learning and realism without dominating decision-making.

IT staff play a critical role during exercise planning and assessment by helping facilitators develop realistic scenarios. Their expertise ensures that system impacts, timelines, and technical constraints reflect plausible incident conditions. This input grounds the exercise in reality, allowing facilitators to tailor technical details to the participant audience.

During exercise execution, IT personnel can serve as observers and, in rare cases, as informational resources rather than decision-makers. They answer questions about system status, data availability, and technical feasibility, helping other participants understand constraints and tradeoffs. However, they do not direct actions or attempt to "fix" the incident during the exercise. In most cases, the IT personnel observe.

This separation of roles reinforces Strategic Doing skills by allowing non-IT participants to focus on organizational priorities, coordination, and accountability, while IT staff provide technical grounding without driving decisions. The result is a more authentic representation of how cyber incidents unfold across organizations, along with a learning environment that engages all participants meaningfully.

In some deployments, IT participation is further expanded through the integration of the IT-centric CySIM, enabling parallel technical and organizational exercise tracks.

Cross-Organizational CIME: Integrated Technical and Organizational Exercises

While CIME is intentionally designed to center non-IT participants and organizational decision-making, many real-world incidents require technical teams to operate concurrently. To support this reality, the CIME framework can be paired with CySIM in a CO-CIME (Cross-Organizational CIME) to create an integrated exercise model that engages both technical and non-technical participants in parallel.

CySIM is a technical cybersecurity exercise that focuses on system-level analysis, incident response, and the operational constraints faced by IT staff during an incident. When combined with CIME, CySIM enables a dual-track exercise structure in which IT participants address technical challenges while business operations participants simultaneously manage organizational impact, communication, and continuity decisions.

In a CO-CIME configuration, the two tracks are intentionally interdependent. Information generated by IT teams, such as system availability, data integrity, or projected recovery timelines, feeds into the business operations discussions as evolving constraints rather than solutions. Conversely, organizational priorities and decisions emerging from business operations teams shape the context in which IT teams operate. This structure mirrors real incident dynamics, where technical and organizational responses proceed in parallel but remain tightly coupled.

From an educational perspective, the CO-CIME model reinforces role clarity and socio-technical systems thinking. IT participants experience how their actions influence organizational outcomes, while business operations participants gain insight into the uncertainty and tradeoffs inherent in technical response. Importantly, this integration preserves the core pedagogical intent of CIME by preventing technical problem-solving from dominating organizational decision-making.

CySIM and CIME can each be run independently; however, their integration provides a more comprehensive learning experience for advanced audiences, including students, professional responders, and cross-functional teams. This combined approach supports a deeper understanding of cybersecurity incidents as complex, multi-layered events that require coordinated technical and organizational action.

6. Strategic Doing as the Action-Oriented Pedagogical Core of CIME

Cybersecurity tabletop exercises often conclude with after-action discussions or lists of recommended controls. While these artifacts can be informative, they frequently fail to translate into sustained organizational change or measurable learning outcomes. To address this limitation, Cybersecurity Incident Management Exercises (CIME) explicitly integrate Strategic Doing [8, 9] as the mechanism that transforms scenario discussion into actionable learning and organizational follow-through.

Strategic Doing is a discipline for taking effective action in complex, uncertain situations by bringing the right people together to focus on shared outcomes, leverage existing assets, and move forward through short, learning-based action cycles rather than long-range or idealized plans. Instead of asking “What’s the perfect solution?”, Strategic Doing asks four practical questions: What could we do? What should we do? What will we do? How will we learn together? This creates clarity, momentum, and accountability even when information is incomplete. Strategic Doing mirrors both the reality of cyber incidents and the professional decision-making environments in which engineers operate, where diverse roles must communicate clearly, make decisions under pressure and with incomplete information, and learn their way forward together while sustaining operations and trust.

Embedding Strategic Doing Within the CIME Process

Strategic Doing is embedded in CIME throughout both the exercise execution and post-exercise phases. As participants work through the scenario, facilitators guide teams to move beyond reactive discussion and instead engage in a structured decision-making process centered on the four core questions:

1. **What could we do?**
   Participants identify available resources, brainstorm ways they might be linked and leveraged to address the scenario, and list potential actions to sustain operations, protect people, communicate with stakeholders, and manage uncertainty within the constraints imposed by the incident.
2. **What should we do?**
   Teams evaluate and prioritize these potential actions based on mission impact, feasibility, time sensitivity, and organizational capacity rather than technical idealism.
3. **What will we do?**
   By choosing the first actions the team believes will be most helpful, participants commit to a small number of concrete, near-term actions that can realistically be executed and that will produce co-created learning needed to build complete solutions, clarifying ownership and coordination needs for each action.
4. **How will we learn together?**
   Teams identify follow-on actions and checkpoints, reinforcing continuity beyond the immediate exercise and acknowledging that incident management is an ongoing process that requires collective learning rather than a discrete event with clear solutions.

This structure supports disciplined decision-making while explicitly acknowledging real-world constraints, including staffing limitations, governance structures, regulatory requirements, and public accountability. It is also repeatable, providing participants with a methodology they can practice and improve over time.

Educational Value of Strategic Doing in Cybersecurity Exercises

From an educational perspective, embedding Strategic Doing within CIME produces several important learning outcomes:

- **Actionable Learning:** Participants leave the exercise with specific, achievable next steps rather than abstract observations or generalized recommendations. The methodology also provides a framework for teams to co-create the new learning needed to address the complex challenges posed by cyber incidents effectively.
- **Socio-Technical Systems Thinking:** Strategic Doing emphasizes that effective cyber incident management necessitates a balanced approach that considers technical, operational, legal, communication, and human factors.
- **Cross-Functional Ownership:** The framework promotes shared responsibility across roles, reinforcing that cybersecurity incidents are organizational challenges rather than solely IT problems. When all members of a response team share a common

understanding of the situation and priorities for responding, they are empowered to take action.
- **Transferable Skills:** The decision-making and collaboration skills practiced through Strategic Doing are applicable beyond cybersecurity incidents, including emergency management, continuity planning, and organizational resilience efforts.

By emphasizing outcomes prioritization, asset-based action, and accountability, Strategic Doing transforms CIME from a discussion-based tabletop exercise into a structured learning experience grounded in experiential and collaborative pedagogy.

Strategic Doing and Post-Exercise Continuity

A distinguishing feature of CIME is that Strategic Doing extends beyond the exercise itself. Outputs generated during the exercise, such as prioritized outcomes, asset-based actions, identified dependencies, and communication considerations, serve as inputs for post-exercise activities. Facilitators use these outputs to support short-term improvement plans, follow-up discussions, targeted training, and iterative refinement of incident management practices.

This continuity reinforces learning retention and helps organizations translate insights gained during the exercise into sustained improvements. Rather than treating the exercise as a one-time event, Strategic Doing positions CIME as part of an ongoing learning and resilience-building process.

7. CIME Exercise Taxonomy

As CIME deployments expanded across sectors and audiences, it became clear that a single exercise format could not effectively support all learning objectives. Differences in participants' backgrounds, organizational affiliations, and role expectations significantly influence how discussions unfold and which learning outcomes are achievable. To address this challenge, we developed a taxonomy to guide facilitators in selecting and adapting CIME structures to align with participant composition and educational goals.

Motivation for a Taxonomy

Cybersecurity incident management exercises are often described as if they are interchangeable, with limited attention paid to how participant composition and role structure shape learning. In practice, however, exercises involving participants from a single organization differ substantially from those conducted with mixed-sector or public audiences. Similarly, asking participants to act in their real-world roles produces different discussions than assigning them fictional or unfamiliar roles.

The CIME taxonomy was developed to make these distinctions explicit. It provides facilitators with a structured way to reason about exercise design choices and their implications for engagement, realism, and learning outcomes. Participant affiliation and role assignment influence the scope of actions teams can realistically commit to during and after the exercise.

Taxonomy Dimensions

The taxonomy consists of two primary dimensions: participant affiliation and role assignment strategy.

Participant Affiliation describes how participants are connected outside the exercise environment:

- **Intra-Organizational.** All participants come from the same organization or entity, such as a city department, school district, or business unit. These exercises emphasize internal coordination, role clarity, and alignment of priorities.
- **Sector-Aligned.** Participants represent various organizations within the same sector, such as agriculture, education, and local government. This format supports discussion of shared dependencies, sector-wide risks, and collaborative response strategies.
- **Cross-Sector or Community.** Participants do not share a common organizational or sector affiliation. These exercises are often used in conferences, public workshops, or awareness-focused settings, emphasizing a broad understanding rather than organization-specific planning.

Role Assignment Strategy defines how participants engage with the scenario:

- **Real-Role Play.** Participants assume the same roles they play in their professional lives. This approach maximizes authenticity and personal investment, particularly for organizational or sector-aligned exercises.
- **Scenario-Based Role Play.** Participants are assigned fictional or alternative roles, such as communications lead or emergency manager. This approach enables participants to explore perspectives they may not typically encounter, which can help balance discussions in mixed groups and often encourages them to participate more freely, deepening their learning and insights.

Taken together, these two dimensions form a 2×3 matrix that captures the most common CIME configurations. For example, an intra-organizational exercise using real role-play may resemble a department-level continuity planning discussion, while a cross-sector exercise using assigned scenario-based roles may prioritize awareness-building and shared vocabulary.

This matrix helps facilitators anticipate the types of discussions that are likely to emerge and select facilitation strategies accordingly. It also supports intentional alignment between exercise design and learning objectives, reinforcing CIME as an educational intervention rather than a one-size-fits-all activity.

The current taxonomy has proven sufficient for the range of CIME deployments conducted to date. It captures key variations in audience composition and role structure while remaining simple enough for practical use. Future extensions could incorporate additional dimensions, such as exercise goal (e.g., awareness building versus continuity planning) or delivery format (e.g., in-person, hybrid, or virtual). However, the two-dimensional taxonomy provides a stable foundation for consistent exercise design and comparative analysis across deployments.

8. Research Context 1: Facilitator Training Program

To support consistent and scalable implementation of CIME, a structured facilitator training program was developed and delivered to 40 participants across multiple cohorts. The training is designed not merely to introduce the CIME framework, but to prepare participants to guide others through the structured decision-making process with fidelity to its pedagogical intent.

The scalability and educational effectiveness of CIME depend heavily on skilled facilitation. Unlike highly scripted technical exercises, CIME requires facilitators to manage group dynamics, maintain focus on organizational decision-making, and ensure that Strategic Doing principles guide discussion rather than allowing conversations to drift toward technical troubleshooting or abstract planning. In this sense, facilitation serves as an instructional control mechanism that maintains the exercise's socio-technical emphasis.

CIME employs a train-the-trainer model to enable distributed delivery across sectors and geographic regions. Facilitators are trained not only in the mechanics of running an exercise, but also in the underlying pedagogy: guiding participants through ambiguity; redirecting discussion toward feasible, asset-based, outcomes-oriented action; reinforcing the assumed-breach framing; and balancing equity of voice with time discipline. As deployments expanded across local government, K–12 education, agriculture, transportation, manufacturing, and other sectors, structured facilitator preparation became essential to maintaining pedagogical consistency while allowing for contextual adaptation.

Following training, facilitators receive a comprehensive toolkit that includes scenario materials, role cards, run-of-show guides, timing aids, and structured note-taking templates. These materials support consistency without imposing rigidity, enabling facilitators to tailor exercises to local contexts, participant experience levels, and available time while preserving core design elements.

To reinforce sustainability and recognize facilitator contributions, CIME incorporates micro-credentials for individuals who complete training and deliver exercises. These credentials support professional development while fostering a shared identity among facilitators across sectors. In several contexts, including agriculture and local government, this distributed model has enabled trusted community members, such as Extension educators, to deliver CIME locally, reducing reliance on centralized delivery and strengthening long-term community engagement.

Through this combination of structured training, adaptable materials, and distributed facilitation, CIME is intentionally designed to remain sustainable beyond a single institution or funding cycle.

Training Structure

The facilitator training is delivered as a five-hour workshop consisting of six integrated components:

1. **CIME Mini-Simulation (45 minutes)**
   Participants experience a condensed CIME exercise as learners.
2. **Foundational Principles of Strategic Doing (35 minutes)**
   Instruction in psychological safety, equity of voice, framing questions, asset-based innovation, decision matrices, and the four questions of agile strategy.
3. **The Elements of CIME (70 minutes)**
   Detailed walkthrough of pre-session preparation, participant selection, role assignment, run-of-show timing, and post-event follow-up.
4. **Facilitation Best Practices (25 minutes)**
   Techniques for guiding discussion, managing time, promoting equity of voice, and maintaining focus on organizational decision-making rather than technical troubleshooting.
5. **Practice Facilitation Simulation (50 minutes)**
   Participants rotate through facilitation roles and guide segments of a CIME simulation themselves.
6. **Reflection and Q&A (25 minutes)**
   Structured discussion of challenges, insights, and implementation considerations.

The training emphasizes experiential learning. Participants do not merely observe a CIME; they actively experience, analyze, and practice facilitating the exercise.

Facilitator training evaluation results

A total of 40 individuals completed facilitator training during the study period. Participants represented diverse professional backgrounds, including:

- Extension and community educators
- Municipal and regional administrators
- IT professionals
- Higher education staff
- Industry representatives
- Graduate students

This diversity reflects the intended cross-sector applicability of the CIME model.

Evaluation Design

At the conclusion of the training, participants completed a structured evaluation instrument consisting of Likert-scale and open-ended questions assessing:

- Clarity of the CIME framework
- Confidence in facilitating a CIME session
- Understanding of Strategic Doing principles
- Perceived preparedness to implement CIME independently
- Overall value of the training experience

Responses were analyzed descriptively, and open-ended responses were reviewed for recurring themes.

Findings

Facilitator feedback indicated a substantial perceived value of the training experience. Participants consistently reported increased confidence in guiding group discussion, improved understanding of the five-step incident management process, and greater appreciation for the importance of facilitation discipline in preventing exercises from reverting to technical troubleshooting.

Open-ended responses revealed several consistent themes:

1. **Clarity of Structure** – Participants valued the explicit run-of-show and timing guidance.
2. **Importance of Psychological Safety** – Many highlighted the importance of equity of voice and safe participation for meaningful discussion.
3. **Shift from Planning to Doing** – Participants noted that the Strategic Doing framework helped move discussions from abstract planning to actionable commitments.
4. **Readiness to Implement** – Several respondents indicated feeling prepared to facilitate CIME sessions within their organizations or communities.

These findings suggest that the facilitator training functions as an instructional control mechanism, helping preserve the pedagogical integrity of CIME as it scales across contexts.

9. Research Context 2: CO-CIME Pilot

To evaluate the applicability of CIME within an engineering education context, a combined CySIM + CIME exercise (CO-CIME) was implemented as a structured classroom pilot involving undergraduate students. This pilot was designed to test whether the dual-track incident model could effectively support interdisciplinary collaboration, socio-technical reasoning, and decision-making under constraint in an academic setting.

Participants and Context

The pilot involved 30 undergraduate students drawn from two academic programs: cybersecurity (technical track) and business (organizational track). Students were organized into 5 tables, each consisting of participants assigned to either an IT response role (CySIM track) or a managerial/leadership role (CIME track). Each table included 5-7 students from a single track (either cybersecurity or business). Professional mentors and observers were present to provide realism and limited guidance but did not direct decision-making.

The exercise was conducted as a four-hour structured simulation. Students were presented with a realistic cyber incident scenario and engaged in parallel decision-making processes reflecting the technical and organizational dimensions of a disruption. The exercise incorporated the five-step incident management process and Strategic Doing methodology described earlier in this paper.

Study Design and Data Collection

To assess the educational impact of the pilot, students completed a post-exercise evaluation instrument consisting of both Likert-scale and open-ended questions. The quantitative item asked students to rate the overall value of the exercise on a 5-point scale (1 = low, 5 = high). Open-ended questions asked students to identify the most valuable aspects of the experience and reflect on their learning.

A total of 22 responses were collected (73% response rate). Of these, 20 provided numeric ratings usable for quantitative analysis.

Quantitative results were analyzed descriptively. Open-ended responses were reviewed and coded thematically to identify recurring patterns in student perceptions and learning outcomes.

Quantitative Results

Students rated the overall value of the CO-CIME experience highly. The mean rating was **4.35 out of 5** (SD ≈ 0.75), with a median of 4.5.

The distribution of ratings is shown below.

Rating (1–5)	Count	Percentage
5	10	50%
4	7	35%
3	3	15%
1–2	0	0%

85% of respondents rated the exercise as 4 or 5. No respondents rated the experience below 3.

These results indicate substantial perceived educational value among participants and suggest that the dual-track structure translates effectively to an undergraduate learning environment.

Qualitative Findings

Open-ended responses revealed several consistent themes aligned with the intended pedagogical goals of CIME.

Cross-Disciplinary Collaboration

Students frequently identified collaboration across technical and non-technical roles as the most valuable aspect of the exercise. Many noted that working with peers from different disciplines broadened their understanding of how cyber incidents affect organizations beyond technical systems.

Representative comments included:

- “Working as a team. It was accurate to the real workplace.”
- “The different perspectives I got from everyone I worked with.”
- “Collaboration and communication.”

These comments suggest that the exercise successfully exposed students to interdisciplinary dynamics reflective of real-world incident response environments.

Communication Under Constraint

Students emphasized the importance of communication during uncertainty. Several noted that managing information flow and coordinating decisions across roles was as challenging as solving technical problems.

One student reflected: “The demonstration of how communication takes resources during an incident was invaluable.”

This aligns directly with the CIME framework's socio-technical emphasis.

Real-World Realism and Decision-Making

Students described the scenario as realistic and valued the opportunity to make decisions under pressure.

Representative comments included:

- “Learning how to think and respond during critical events.”
- “It felt like something that could actually happen.”

These responses indicate that the exercise created an authentic learning environment that extended beyond abstract technical instruction.

Structured Thinking and Role Awareness

Several students commented that they gained clarity about non-IT responsibilities during a cyber incident. Exposure to organizational constraints and leadership perspectives expanded their understanding of how engineering decisions propagate across systems.

Collectively, these qualitative themes demonstrate that the CO-CIME pilot fostered interdisciplinary awareness, structured decision-making, and socio-technical reasoning.

Implications for ECE Education

The classroom pilot provides preliminary evidence that dual-track incident simulations can be integrated into undergraduate engineering education to strengthen professional competencies. Students reported increased appreciation for cross-functional coordination, communication under

uncertainty, and organizational decision-making—skills central to contemporary electrical and computer engineering practice.

For ECE programs, CO-CIME offers a structured mechanism for teaching systems integration in socio-technical environments, aligning with ABET outcomes in teamwork, communication, ethical responsibility, and problem-solving in complex engineering contexts.

While this pilot represents an initial implementation rather than a controlled experimental study, the results suggest that CIME can be effectively adapted from professional training contexts into formal engineering education settings. Future work will expand data collection to include pre- and post-measures.

10. Deployment Case Examples

CIME has been deployed across a range of contexts to support cybersecurity incident management education for diverse audiences. While the specific scenarios, participants, and formats vary, these deployments share a common pedagogical structure grounded in scenario-based learning and Strategic Doing. The examples below illustrate how CIME has been adapted using the exercise taxonomy to support different learning objectives and operational settings.

Local and Regional Government Deployments

CIME has been delivered in conference-style and organizational formats for local and regional government audiences, including elected officials, administrators, and department leaders. These exercises typically emphasize organizational decision-making, public communication, and continuity of essential services rather than technical response. The largest such deployment was at a statewide cybersecurity conference targeted at local governments. We had over 60 participants involved in the CIME.

In these deployments, participants primarily act in their real-world roles, enabling discussions to focus on authority, coordination, and interdepartmental dependencies. Exercises are often conducted in conference settings, allowing participants from multiple jurisdictions to engage in shared learning while recognizing differences in local structure and resources. Observed learning outcomes include improved understanding of non-IT responsibilities during cyber incidents and increased appreciation for cross-functional coordination.

Education and Workforce Development Contexts

CIME has also been used in education-adjacent contexts, including conferences and professional development events that bring together participants from K–12 education, higher education, and related support organizations. In these settings, exercises are often adapted to strike a balance between awareness-building and practical decision-making.

Participants may represent a mix of real-world and scenario-based roles, depending on audience composition. These deployments emphasize shared vocabulary, recognition of organizational dependencies, and the role of leadership and communication during disruption. For educators

and administrators, CIME offers a concrete framework for considering preparedness beyond technical controls.

Sector-Specific Deployments: Transportation and Critical Services

CIME has been adapted for sector-specific audiences where operational continuity and public impact are central concerns. One such deployment involved regional transit authorities, in which the exercise was conducted entirely virtually to accommodate participants who were geographically distributed.

In this context, CIME emphasized decision-making under disruption, coordination across agencies, and communication with external stakeholders. Despite the virtual format, the structured five-step process and Strategic Doing framework supported active participation and meaningful discussion. This deployment demonstrated that CIME can be effectively adapted to virtual environments when facilitation and materials are intentionally designed.

Observations Across Deployments

Across these varied contexts, several consistent patterns emerged. Conference-style CIMEs proved effective for awareness-building and cross-organizational learning, while organizational and sector-specific CIMEs supported more in-depth action planning and follow-up activities. Regardless of format, exercises that aligned participant composition with appropriate role-assignment strategies guided by the CIME taxonomy achieved the intended learning outcomes more consistently.

While most CIME deployments to date have occurred in in-person or conference settings, emerging virtual deployments suggest opportunities for further adaptation. Virtual CIME formats introduce new facilitation considerations but also expand access and scalability. These modalities represent an area for future development and study. Together, these deployments demonstrate that CIME is adaptable across contexts, scales, and delivery modalities while preserving its core pedagogical structure.

11. Lessons Learned from CIME Deployments

Deploying Cybersecurity Incident Management Exercises (CIME) across diverse sectors, including local government, K–12 education, agriculture, and industry, has yielded consistent observations on participant learning, facilitation, and organizational readiness. These lessons emerged across multiple exercise formats and participant configurations and provide insight into how CIME functions as an educational intervention rather than solely a preparedness activity.

Participants Initially Default to Technical Thinking

Across nearly all deployments, non-IT participants initially expected IT staff to "solve" the incident, even when explicitly informed that technical remediation was not immediately available. Early discussions often focused on restoring systems or identifying technical fixes,

rather than addressing operational continuity or organizational impact. This pattern reflects how deeply technical-centric narratives of cybersecurity are embedded within many organizations.

The structured use of Strategic Doing proved essential in redirecting discussion toward decision-making, coordination, and communication. As exercises progressed, participants increasingly recognized their own responsibilities in managing through disruption. This shift from viewing cybersecurity incidents as technical problems to organizational challenges represented a significant learning outcome.

Strategic Doing Shifts Focus from Ideal Solutions to Feasible Actions

A recurring observation was participants' tendency to propose actions that assumed additional resources, expanded authority, or future investments. While these ideas were often reasonable in principle, they did not reflect the constraints typically faced during an active incident.

Strategic Doing provided a disciplined mechanism to refocus teams on actions that could realistically be taken with existing capabilities. Over the course of the exercise, many groups demonstrated a measurable transition from aspirational planning toward pragmatic commitment. This shift toward feasibility and prioritization distinguishes CIME outcomes from traditional tabletop exercises, which often conclude with generalized recommendations.

Cross-Functional Dialogue Improves Shared Understanding

CIME consistently surfaced gaps in understanding between technical and non-technical participants regarding system dependencies, decision authority, and communication expectations. Without structure, these gaps can lead to unproductive discussion or misplaced assumptions during real incidents.

When guided by Strategic Doing, cross-functional dialogue became more focused and productive. Teams were required to align on priorities and next steps rather than debate abstract roles or responsibilities. Participants frequently reported increased appreciation for the constraints and perspectives of other functions, reinforcing the value of interdisciplinary engagement in cybersecurity education.

Facilitation Is Critical to Learning Outcomes

The effectiveness of CIME as a learning experience depends heavily on skilled facilitation. Facilitators play a central role in maintaining focus on organizational decision-making and action rather than allowing discussions to drift toward technical detail or checklist-driven thinking.

Deployments supported by trained facilitators and standardized toolkits achieved intended learning outcomes more consistently. Exercises led by less experienced facilitators were more likely to revert to technical problem-solving. These observations underscore the significance of the train-the-trainer model in ensuring pedagogical consistency while enabling exercises to be tailored to local contexts.

Learning Extends Beyond the Exercise Itself

Organizations that engaged in post-exercise follow-up, such as brief planning meetings, targeted training sessions, or additional exercises, demonstrated stronger retention of insights and a higher likelihood of implementing identified actions. Outputs generated through Strategic Doing, including prioritized and asset-based actions, identified dependencies, and co-created learning within teams, provided a natural bridge between the exercise and these follow-on activities.

This pattern reinforces the importance of viewing CIME as part of an ongoing learning and resilience-building process rather than a one-time event. When integrated into broader training and planning efforts, CIME supports sustained organizational improvement and deeper learning over time.

12. Implications for Engineering and Cybersecurity Education

Cybersecurity education has traditionally emphasized technical proficiency, including secure system design, threat detection, and incident response procedures. While these skills remain essential, findings from CIME deployments suggest that technical competence alone is insufficient to prepare students and professionals to manage real-world cyber incidents. Cyber disruptions unfold within complex socio-technical systems that require coordination, judgment, communication, and adaptive leadership across organizational roles.

CIME offers a replicable educational model for addressing this gap. By framing cyber incidents as organizational disruptions and embedding Strategic Doing within scenario-based exercises, CIME enables participants to practice a proven methodology for decision-making under uncertainty, prioritizing competing demands, and collaborating across functional boundaries. These competencies align closely with broader engineering education goals, including systems thinking, ethical responsibility, and professional readiness.

Teaching Cybersecurity as a Socio-Technical Discipline

One of the most significant educational implications of CIME is its explicit treatment of cybersecurity as a socio-technical discipline. Participants experience firsthand how technical failures propagate into operational, legal, financial, and reputational consequences. This perspective challenges students and professionals to move beyond narrow technical optimization and consider the broader context in which engineering decisions are made.

For engineering and cybersecurity programs, CIME offers a structured approach to introducing socio-technical complexity without requiring deep technical specialization from all participants. Exercises can be adapted to undergraduate, graduate, or professional audiences, allowing learners at different stages to engage meaningfully with cybersecurity incident management.

Developing Decision-Making and Adaptive Leadership Skills

CIME emphasizes decision-making under constraint rather than idealized planning. Through Strategic Doing, participants learn to identify feasible actions, commit to near-term steps, and

reassess priorities as conditions evolve. These skills are directly transferable to engineering practice, where professionals routinely operate under uncertainty, limited resources, and incomplete information.

Embedding this type of action-oriented decision-making into cybersecurity education helps prepare learners for leadership roles, even when they are not the most technically senior individuals in an organization. This is particularly important as engineers and technologists are increasingly expected to contribute to organizational resilience and crisis response.

Integrating CIME into Educational and Professional Contexts

CIME can be incorporated into a variety of educational settings. In academic programs, it can serve as a capstone activity, a module within cybersecurity or systems courses, or a co-curricular experience that brings together students from different disciplines. In professional and continuing education contexts, CIME supports workforce development by engaging both technical and non-technical participants in shared learning experiences.

The taxonomy developed for CIME further supports educational integration by allowing instructors and facilitators to intentionally select exercise formats that align with learning objectives and participant composition. This flexibility enables consistent educational outcomes while accommodating diverse audiences and institutional constraints.

Bridging Education, Practice, and Community Engagement

Finally, CIME demonstrates how cybersecurity education can extend beyond the classroom to support community engagement and workforce preparedness. Deployments involving local governments, schools, agriculture, and industry demonstrate how educational institutions can serve as conveners, fostering shared understanding and capacity-building across sectors.

For engineering educators, this model aligns with broader goals of experiential learning, civic engagement, and applied scholarship. By engaging learners in realistic, consequence-driven scenarios, CIME helps bridge the gap between academic instruction and the complex realities graduates will encounter in professional practice.

13. Conclusion and Future Work

Cybersecurity incidents increasingly disrupt organizations in ways that extend well beyond technical systems, affecting operations, leadership decision-making, and public trust. Traditional cybersecurity exercises, while valuable for testing technical controls, often fail to adequately prepare organizations to manage prolonged disruptions and coordinate across functional roles. This paper introduced Cybersecurity Incident Management Exercises (CIME) as a scenario-based educational framework designed to address this gap.

CIME reframes cyber incidents as organizational challenges and emphasizes co-created learning through collaboration, action, and reflection. By assuming that a breach has already occurred and embedding Strategic Doing within the exercise structure, CIME enables participants to practice

prioritization, communication, and decision-making under constraint. The framework's separation of technical remediation from operational management allows non-IT participants to engage meaningfully, while still grounding scenarios in technical realism.

This work contributes to engineering and cybersecurity education in several ways. First, it presents a repeatable and scalable educational framework that supports experiential learning across sectors and participant backgrounds. Second, it introduces a taxonomy that guides intentional exercise design and facilitates alignment between participant composition and learning objectives. Third, it provides insights from multi-sector deployments that demonstrate how CIME supports learning outcomes related to socio-technical systems thinking, adaptive leadership, and organizational resilience.

Future work will focus on several areas. From a research perspective, ongoing efforts will examine learning outcomes more systematically, including longitudinal studies of how participation in CIME influences organizational practices and individual decision-making over time. Additional work will explore how variations in exercise format, participant affiliation, and facilitation approach affect learning and engagement.

From an educational standpoint, future deployments will expand the integration of CIME into academic curricula, professional education, and community-based training programs. This includes further development of facilitator training materials, refinement of post-exercise follow-up activities, and deeper integration with complementary technical exercises such as CySIM. Together, these efforts aim to strengthen the role of experiential, action-oriented learning in preparing engineers and cybersecurity professionals to operate effectively within complex, real-world environments.

As cyber incidents continue to challenge organizations across sectors, educational approaches that emphasize coordination, judgment, and adaptability will become increasingly important. CIME provides a practical and extensible model for addressing these needs, bridging technical expertise with organizational preparedness and reinforcing cybersecurity as a shared responsibility. CIME demonstrates that cybersecurity education can move beyond technical proficiency toward preparing engineers and professionals to manage disruption, uncertainty, and organizational responsibility, which are capabilities increasingly central to engineering practice.

Appendix A: Representative CIME Run of Show

Cybersecurity Incident Management Exercises (CIME) are intentionally designed to be adaptable to different audiences, settings, and learning objectives. While all CIME deployments follow a common pedagogical structure centered on scenario-based learning and Strategic Doing, the detailed execution flow, including timing, regroup points, and depth of discussion, varies by exercise type. This appendix presents a representative run of show drawn from deployed organizational and conference-based CIME exercises to illustrate how the framework is operationalized in practice.

A.1 Purpose and Scope

The purpose of this appendix is to provide a concrete example of how a CIME unfolds during facilitation while reinforcing that timing and structure are modular. Facilitators adjust pacing and emphasis for different formats, such as organizational exercises, conference sessions, or abbreviated "CIME of One" experiences designed for public or awareness-focused audiences.

A.2 Participant Orientation and Team Setup

CIME exercises begin with participant orientation and team formation. Participants are assigned role-playing identities specific to the cyber incident scenario and briefed on the exercise's goals, emphasizing that the purpose is learning and preparation rather than evaluation or critique. Teams typically also assign three functional roles to support the exercise process:

- **Group Guide**, responsible for keeping the discussion focused and ensuring equitable participation
- **Time Keeper**, responsible for monitoring time and helping the group move between steps
- **Info Keeper**, responsible for capturing key discussion points, decisions, and action items

These functional roles support inclusive participation and reinforce the collaborative nature of the exercise.

A.3 Scenario Introduction

The exercise scenario is introduced through a short video or narrative briefing that presents a cyber incident or cascading disruption that has already occurred [9]. Participants are encouraged to view the scenario from the perspective of their assigned role and to reflect on what is important to them, what systems or services are affected, and who they would need to communicate with under these conditions.

To support comprehension, scenario materials are often presented more than once, and participants are encouraged to take notes prior to group discussion.

A.4 Five-Step Incident Management Process

The core of the CIME follows the five-step incident management process described in the main body of the paper. A representative timeline for an organizational CIME is shown in Table A.1.

Table A.1. Representative CIME Run of Show (Organizational Format)

Phase	Activity	Typical Time	Notes
Orientation	Roles, team functions, exercise framing	5–10 minutes	Shortened for conference formats
Scenario Intake	Video and individual reflection	~10 minutes	Often viewed twice
Step 1	Problem Statement (Current State)	~5 minutes	Establishes shared framing
Step 2	Priorities (Now and Near Term)	~10 minutes	Key decision pivot
Step 3	What Could We Do? (Assets & Options)	~15 minutes	Asset-based brainstorming
Step 4	What Should We Do? (Prioritization)	~15 minutes	Evaluation of ease and impact
Step 5	Action Plan	~15 minutes	Sequencing and ownership
Debrief	Reflection and insights	10–20 minutes	Often expanded

While the structure remains consistent, facilitators may adjust the pace of individual steps based on participants' experience, exercise goals, and available time. Table 2 shows typical times for the three CIME formats.

Table A.2. Representative Timing Variations Across CIME Formats

Exercise Phase	Organizational CIME	Conference CIME	“CIME of One”
Orientation & Roles	5–10 min	5 min	2–3 min
Scenario Intake	~10 min (video twice)	5–7 min (video once)	3–5 min (narrative summary)
Step 1: Problem Statement	~5 min	5 min	3–5 min
Step 2: Priorities	~10 min	5–7 min	5 min

Exercise Phase	Organizational CIME	Conference CIME	“CIME of One”
Step 3: What Could We Do?	~15 min	5–10 min (assets only)	5–7 min
Step 4: What Should We Do?	~15 min	5 min (abbreviated)	5 min (abbreviated)
Step 5: Action Plan	~15 min	— or 5 min	—
Debrief & Reflection	10–20 min	10 min	5 min
Total Duration	**~90–120 min**	**~45–60 min**	**~45-60 min**

A.5 Regrouping and Reflection

Many CIME formats incorporate regroup points where teams briefly share insights, sample problem statements, or priorities with the broader group. These moments reinforce shared learning and help participants recognize common challenges and patterns across teams.

The exercise concludes with a facilitated debrief focused on reflection rather than performance. Participants are asked to identify insights, discuss communication considerations, and reflect on how the exercise informs future preparedness and organizational practices.

A.6 Adaptability Across Exercise Types

The run of show presented here reflects a full organizational CIME. In contrast:

- **Conference CIME sessions** often emphasize early-stage sense-making and prioritization, with abbreviated action planning.
- **CIME of One** experiences focus on individual reflection and awareness, typically emphasizing Steps 1–3 rather than full action planning.

This adaptability enables CIME to support a diverse range of educational and professional contexts while maintaining its core pedagogical structure.