Complication Cards

Activity 3: AI-Assisted Incident Response

How to Use These Cards

During Phase 3 (Response Execution), inject complications every 5 minutes to simulate the dynamic nature of real incidents. Start with milder complications and escalate as appropriate.

Tips:

- Read the complication aloud to the team
- Give them 30 seconds to react before moving on
- Don't inject complications if a team is already struggling
- The goal is adaptation practice, not team breakdown

Grades 9-12: Enterprise Complications

Communication Pressure

COMPLICATION: Media Attention

Situation:

A local news outlet just tweeted: "Sources confirm major cyber incident at TechCorp. Developing story."

Your phone is ringing—it's the communications VP asking for talking points in 5 minutes.

Questions for the team:

- What can you say publicly right now?
- What must you NOT say?
- Who approves external communications?

COMPLICATION: Executive Demand

Situation:

The CEO just sent a message: "I have a board call in 20 minutes. I need a one-paragraph summary of what's happening and whether we're going to make Friday's deadline."

Questions for the team:

- What's the honest answer about the deadline?
- How do you balance transparency with uncertainty?
- What must the CEO understand before the board call?

Scope Expansion

COMPLICATION: New Systems Compromised

Situation:

SentinelAI just flagged additional alerts:

- 12 workstations in the FINANCE network segment
- Same indicators as manufacturing floor
- Finance systems contain payroll and vendor data

Questions for the team:

- Does this change your containment strategy?
- Do you need to notify additional stakeholders?
- What's the new scope of potential data exposure?

COMPLICATION: OT System Alert

Situation:

The HVAC-CONTROLLER-01 (OT/IT bridge system) just showed unusual network traffic. Manufacturing floor temperature is critical for equipment.

If you isolate this system: Risk of equipment damage from temperature fluctuation If you don't isolate: Risk of OT network compromise

Questions for the team:

- How do you balance physical equipment risk vs. cyber risk?
- Who needs to be involved in this decision?
- Is there a middle-ground option?

Human Factors

COMPLICATION: Insider Concern

Situation:

HR just informed you that the employee who clicked the phishing email (jsmith) was recently passed over for a promotion and has been vocal about dissatisfaction.

Questions for the team:

- Does this change your investigation approach?
- How do you handle this sensitively while maintaining security?

- What's the difference between accident and malice?

COMPLICATION: Stakeholder Conflict

Situation:

The Manufacturing VP just called: "I don't care about your security concerns—we have a $2M order shipping Friday and you want to shut down my floor? I'll take this to the CEO."

Questions for the team:

- How do you maintain security posture while addressing business needs?
- What options might satisfy both security and operations?
- When do you escalate vs. compromise?

Grades 6-8: School Complications

Communication Pressure

NEW DEVELOPMENT: Parent Group

Situation:

A parent posted on Facebook: "Anyone else hearing about a computer problem at Riverside? What aren't they telling us??"

The post already has 47 comments and the principal wants a response NOW.

Questions for the team:

- What can you share publicly?
- Who should respond—and how?
- How do you prevent rumors while investigation continues?

NEW DEVELOPMENT: Media Inquiry

Situation:

A local TV station just called the front office asking for a statement about "the cyber attack at Riverside Middle School."

The principal needs talking points in 2 minutes.

Questions for the team:

- Should you confirm or deny an "attack"?
- What's the difference between "incident" and "attack"?
- What do you say when you don't know everything yet?

Scope Changes

NEW DEVELOPMENT: Spread to Other Classrooms

Situation:

Two more classrooms just reported the same symptoms—pop-ups on their computers.

The problem is spreading.

Questions for the team:

- Does this change your response priority?
- Should you shut down the whole school network?
- How do you balance learning disruption vs. containment?

NEW DEVELOPMENT: Student Data Concern

Situation:

A teacher just realized that the affected file server also contains student contact information and emergency contacts.

This might be a data breach, not just malware.

Questions for the team:

- Who needs to be notified if student data was accessed?
- Are there legal requirements you need to consider?
- How does this change stakeholder communication?

Human Factors

NEW DEVELOPMENT: The Student Who Clicked

Situation:

You've identified the student who clicked the phishing email. They're crying in the hallway, saying "I ruined everything."

Questions for the team:

- Is this a discipline issue or a learning opportunity?
- How do you balance investigation with compassion?
- What message do you want to send to all students?

NEW DEVELOPMENT: Teacher Resistance

Situation:

A teacher refuses to stop using computers: "I have a major lesson today and I won't let some pop-ups ruin my teaching. The kids need their projects."

Questions for the team:

- Can you force compliance? Should you?
- What's the risk if they keep using infected systems?
- How do you balance authority with cooperation?

Grades 3-5: Mystery Complications

BREAKING NEWS!

Situation:

Another classroom just reported the same problem—pop-ups on their computers too!

Questions for the team:

- Is the problem spreading?
- What should those students do?
- Should we check all the classrooms?

BREAKING NEWS!

Situation:

The student who clicked the email is really upset. They didn't mean to cause problems!

Questions for the team:

- Is it their fault?
- How can we make them feel better?
- What should everyone learn from this?

BREAKING NEWS!

Situation:

Parents are starting to call the school asking what's happening with the computers.

Questions for the team:

- What should we tell the parents?
- Should we tell them everything or wait until we know more?
- Who should talk to the parents?

Grades K-2: Fix It Team Surprises

SURPRISE!

Situation:

After we turned on the computers, one of them still won't work!

Questions for the class:

- Should we try the same fix again?
- Maybe there's a different problem?
- Who should we ask for help?

SURPRISE!

Situation:

A student says they saw someone turn off the switch before. Maybe it wasn't an accident!

Questions for the class:

- Does it matter who turned it off?
- Should we find out what happened?
- What's most important—fixing it or finding out why?

From "True Teamwork: Building Human-AI Partnerships" — NICE K12 2025 Dr. Ryan Straight, University of Arizona • ryanstraight@arizona.edu