Nonprofit Crisis Response Tabletop Exercises

Exercise Context: Midwest Youth Education Alliance (MYEA)

Organization Profile:

- Annual Budget: $625,000
- Staff: 12 full-time, 8 part-time
- Location: Minneapolis, MN
- Mission: After-school education programs for underserved youth
- Programs: STEM Education, Literacy Support, College Prep

Scenario 1: The Sudden Grant Freeze

Initial Setup

Friday, 4:45 PM: Development Director Sarah Chen receives an email from Minnesota Department of Education Program Officer James Martinez: The $250,000 "Youth STEM Success" grant will be suspended in 30 days due to state budget cuts. This grant funds your flagship robotics program serving 150 students across five schools and covers salaries for three full-time STEM educators.

Phase 1: Immediate Crisis Management (Days 1-3)

Situation Details:

- Three STEM teachers (Marcus Washington, Priya Patel, and David Kim) are fully grant-funded
- Current robotics program mid-semester with upcoming state competition
- $45,000 in recently purchased robotics equipment
- Partner schools: Lincoln Middle School, Washington Tech, Roosevelt STEM Academy

Injects:

1. Lead teacher Marcus Washington emails at 8 PM asking if he should start job hunting
2. Channel 5 education reporter Emma Rodriguez requests comment by 9 AM
3. Your primary bank contact, Thomas Wright at First Community Bank, demands updated financial plan
4. Roosevelt STEM Academy Principal Dr. Janet Foster calls about competition preparations

Discussion Points:

- Immediate staffing decisions for STEM team
- Competition commitments ($12,000 already paid in fees)
- Equipment lease obligations
- Partner school communications

Technical Tasks:

- Review grant compliance requirements
- Analyze current program expenses
- Map affected stakeholders

Phase 2: Stakeholder Management (Days 4-14)

Situation Details:

- Board Chair Victoria Martinez calls emergency meeting
- Parent-Teacher Association President Robert Chang demands answers
- Major donor ($50,000/year) Michael Davidson threatens to withdraw support
- 150 student families need program status updates

Injects:

1. Board Treasurer Kevin O'Brien identifies potential reserve fund violations
2. Competition organizer needs confirmation of participation
3. Local tech company CEO Lisa Zhang offers potential emergency support
4. Three STEM program students qualify for national competition

Discussion Points:

- Program transition timeline
- Emergency funding sources
- Competition participation decision
- Equipment disposition plan

Technical Tasks:

- Create stakeholder communication matrix
- Develop program wind-down timeline
- Draft emergency funding proposals

Phase 3: Strategic Restructuring (Days 15-30)

Situation Details:

- Local tech startup TechForward offers program adoption
- Competing nonprofit suggests merger
- Foundation contact suggests converting to fee-based model

Injects:

1. Staff present alternative funding proposal
2. Partner school Roosevelt STEM offers shared cost model
3. State Senator Maria Rodriguez requests impact statement
4. Parent group proposes crowdfunding campaign

Discussion Points:

- Program sustainability options
- Partnership opportunities
- Staff retention strategies
- Equipment utilization plan

Technical Tasks:

- Draft 12-month financial scenarios
- Create program transition plan
- Develop new funding model

Scenario 2: The Digital Safety Crisis

Initial Setup

Following MYEA's public support for enhanced student mental health resources and anti-bullying initiatives, the organization faces coordinated online harassment targeting staff and youth programs.

Phase 1: Immediate Protection (Hours 0-24)

Situation Details:

- Executive Director's professional contact information compromised
- IT Manager Kevin Wu discovers coordinated website attacks
- Communications Director Maya Singh's work email flooded with threats
- Three program locations received concerning messages

Injects:

1. Anonymous threat references staff members' families
2. Cybersecurity firm detects attempted database breach
3. Partner school Principal Sarah Martinez reports student safety concerns
4. Program coordinator's professional accounts compromised

Discussion Points:

- Staff security protocols
- Digital asset protection
- Law enforcement coordination
- Student safety procedures

Technical Tasks:

- Document all incidents
- Secure digital infrastructure
- Enable enhanced monitoring
- Contact cybersecurity support

Phase 2: Crisis Communication (Days 2-7)

Situation Details:

- Local education advocacy groups offer support
- Media requesting statement about threats
- Partner schools demand safety protocols
- Board members receiving concerning messages

Injects:

1. News outlet requests interview about "student safety measures"
2. Major donor Beth Williams questions program security
3. Partner organization reports similar incidents
4. Staff member reports suspicious activity near program site

Discussion Points:

- Media response strategy
- Staff support systems
- Program security protocols
- Partner communications

Technical Tasks:

- Implement crisis communications
- Document incident timeline
- Review security procedures
- Set up monitoring systems

Phase 3: Long-term Resilience (Week 2-4)

Situation Details:

- Security audit reveals infrastructure gaps
- Staff requesting enhanced safety measures
- Insurance provider requires protocol updates
- Similar organizations offer collaborative security solutions

Injects:

1. Security consultant John Chen provides vulnerability assessment
2. HR Director Patricia Moore reports increased staff concerns
3. Insurance provider mandates safety improvements
4. Education network offers shared security resources

Discussion Points:

- Future security protocols
- Staff safety guidelines
- Facility access procedures
- Partnership opportunities

Technical Tasks:

- Update security policies
- Implement monitoring systems
- Create incident response playbook
- Train staff on new procedures

Scenario 3: The Student Data Privacy Challenge

Initial Setup

Tuesday, 10:15 AM: MYEA receives a federal subpoena demanding student records from 2021-2024, specifically targeting participants in your academic support and counseling programs. The subpoena arrives following a state senate hearing about youth privacy protection.

Phase 1: Legal Assessment (Hours 0-48)

Situation Details:

- Database contains 2,300 student records with sensitive information
- Database administrator Jenny Martinez on medical leave
- Board includes two attorneys: Mark Davidson (Corporate) and Lisa Chen (Education Law)
- Recent database migration incomplete

Injects:

1. Board member Mark Davidson emphasizes compliance requirements
2. Board member Lisa Chen raises student privacy concerns
3. Database provider needs access authorization
4. Major donor Eleanor Wright inquires about data protection
5. IT contractor discovers unauthorized backup files

Discussion Points:

- Legal obligations under FERPA
- Student privacy commitments
- Data access protocols
- Legacy system management

Technical Tasks:

- Audit privacy policies
- Map data storage locations
- Review vendor agreements
- Document access protocols

Phase 2: Stakeholder Response (Days 3-7)

Situation Details:

- Local media investigating student privacy story
- Program Director Sam Taylor concerned about family confidentiality
- Partner organizations facing similar challenges
- Parent advisory meeting scheduled

Injects:

1. Education law specialist offers consultation
2. News outlet publishes privacy concern story
3. Corporate partners request security briefing
4. School district superintendent requests meeting
5. Internal memo leaked to social media

Discussion Points:

- Legal response strategy
- Stakeholder management
- Media coordination

- Student protection measures

Technical Tasks:

- Prepare family communication
- Document legal guidance
- Review protection measures
- Create response matrix

Phase 3: Policy Strengthening (Weeks 2-4)

Situation Details:

- Board establishes privacy committee
- Technology assessment recommends updates
- Staff requests clear guidelines
- Similar cases emerging nationally

Injects:

1. Board treasurer requests policy revision
2. IT audit reveals security gaps
3. Education partners require new protocols
4. State association requests best practices
5. Insurance updates privacy requirements

Discussion Points:

- Privacy framework updates
- Staff training needs
- Vendor protocols
- Partnership standards

Technical Tasks:

- Draft privacy policies
- Implement security controls
- Create response procedures
- Develop training program

Scenario 4: The Data Breach

Initial Setup

Saturday, 8:30 PM: IT coordinator Peter Chang discovers unauthorized access to your student and donor database. Investigation suggests the breach began during your annual education fundraiser three months ago. The database contains sensitive information for 8,000 individuals, including students, families, and supporters.

Phase 1: Incident Response (Hours 0-24)

Situation Details:

- Payment system flags suspicious activity
- Board Chair's financial information compromised
- Development office loses database access
- Annual compliance review approaching

Injects:

1. IT team discovers malware in administration systems
2. Multiple stakeholders report suspicious activity
3. Payment processor issues security alert
4. Backup systems show irregularities
5. Staff member identifies potential security breach point

Discussion Points:

- System protection priorities
- Investigation scope
- Reporting requirements
- Insurance procedures

Technical Tasks:

- Create incident timeline
- Secure affected systems
- Begin impact assessment
- Document compromised data

Phase 2: Impact Management (Days 2-7)

Situation Details:

- 3,000 financial records potentially exposed
- Financial institutions report concerns

- Annual report deadline approaching
- State notification requirements triggered

Injects:

1. Cybercrime unit requests briefing
2. Financial partner raises liability concerns
3. Insurance requires documentation
4. Security firm discovers data exposure
5. Additional systems compromised

Discussion Points:

- Notification priorities
- Legal implications
- Resource allocation
- Investigation coordination

Technical Tasks:

- Prepare notifications
- Document affected systems
- Implement security measures
- Create communication plan

Phase 3: Recovery & Prevention (Weeks 2-8)

Situation Details:

- Audit reveals multiple vulnerabilities
- Remote work creates security challenges
- Insurance requires security upgrades
- Board requests security oversight

Injects:

1. Systems require critical updates
2. Unauthorized access continues
3. Security upgrades exceed budget
4. Partner organizations report breaches
5. Regulatory review scheduled

Discussion Points:

- Security enhancement priorities
- Budget reallocation needs
- Policy updates
- Training requirements

Technical Tasks:

- Update infrastructure
- Implement new controls
- Develop training program
- Create monitoring system

After-Action Review Template

[Previous template remains the same]

Scoring Matrix

[Previous matrix remains the same]