Disaster Planning and Incident Handling using Gaming Concepts

Michael Solomon, Ph.D.

June 2017
Your speaker

- **Michael Solomon, Ph.D.**
  
  CISSP PMP CISA

- **Solomon Consulting Inc.**
  
  - OpenEdge, Roundtable, Security architecture
    - Since 1988 (Progress Version 4)
  
  - CyberSecurity Simulation attack team leader
    - Penetration testing, attack detection and response

- **Emory University**
  
  - Assured Information Management and Sharing (AIMS)
  
  - Private location proximity detection research

- **University of the Cumberlands**
  
  - Associate Professor, Master of Science in Information Systems Security program
Agenda

- Active learning – why bother?
- Can gaming really help with the boring stuff?
- What will it do for me?
- OK, “I want to go to there”
  - Liz Lemon
You’ve heard this before

Two easy steps:
1) Make a plan
2) Follow the plan
Question 1:
Do you have a written BCP/IRP?
Responding to incidents is all about minimizing surprise and confusion.
### Emergency Procedures

#### Challenge: Engine Failure During Takeoff Roll
- **Throttle**: IDLE
- **Brakes**: APPLY
- **Wing Flaps**: RETRACT
- **Mixture**: IDLE CUT-OFF
- **Fuel Shutoff Valve**: PULL OFF
- **Magnetos Switch**: OFF
- **Master Switch**: OFF

#### Challenge: Engine Failure Immediately After Takeoff
- **Airspeed**: (flaps up) 65 KIAS
- **Mixture**: IDLE CUT-OFF
- **Fuel Shutoff Valve**: PULL OFF
- **Magnetos**: OFF
- **Wing Flaps**: AS REQUIRED
- **Master Switch**: OFF

#### Challenge: Engine Failure in Flight
- **Trim for Best Glide**: 65 KIAS
- **Pick Suitable Landing Site**
- **Fly Toward Landing Site**
- **Fuel Selector**: BOTH
- **Fuel Shutoff Valve**: IN
- **Mixture**: AS REQUIRED
- **Fuel Pump**: ON
- **Magnetos**: ON / BOTH

### Cessna 172R Checklist

#### Challenge: Engine Fire in Flight
- **Mixtures**: IDLE CUT-OFF
- **Fuel Shutoff Valve**: OFF / PULL OUT
- **Fuel Pump**: OFF
- **Vents Heat / Air**: CLOSED
  (except wing root vents)
- **Airspeed**: 100 KIAS
  (If fire is not extinguished, increase glide speed to find an airspeed which will provide an incombustible mixture.)
- **Forced Landing**: EXECUTE
- **SEE ENGINE FAILURE IN FLIGHT: NO RESTART CHECKLIST**

#### Challenge: Electrical Fire in Flight
- **Magnetos**: OFF
- **All Other Switches Except Ignition**: OFF
- **Vents Heat / Air**: CLOSED
- **Fire Extinguisher**: ACTIVATE
  - **WARNING**: AFTER DISCHARGING FIRE EXTINGUISHER WITHIN CLOSED CABIN, VENTILATE CABIN
  - **IF FIRE APPEARS OUT AND ELECTRICAL POWER IS NECESSARY FOR CONTINUANCE OF FLIGHT**
- **Master Switch**: ON
- **Circuit Breakers / Electrical Switches**: check for faulty circuit, do not reset
  - **Radio**: ON
  - **One at a time, with delay after each until short circuit is localized.**
- **Vents Heat / Air**: OPEN
  (When it is ascertained that fire is completely extinguished.)
Response success depends on the quality of your plan and the readiness of your team.
Let's plan
Why am I in this meeting?

Boring!

What a waste of time.
Question 2:

“Surprise incidents” list
Question 3:
“Surprise incidents” list
Take 2
Question 2: Functional areas

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Network</td>
</tr>
<tr>
<td>2</td>
<td>Data center</td>
</tr>
<tr>
<td>3</td>
<td>Physical plant</td>
</tr>
<tr>
<td>4</td>
<td>Customer facing web application</td>
</tr>
</tbody>
</table>
Let’s review our questions

Question 1
• No engagement
• Raise your hands

Question 2
• Limited engagement with competition

Question 3
• Enhanced engagement
• Assigned roles
• Incentive (candy!!)
Which one was most effective?
It’s all a game.
Active learning and engagement fosters critical thought and ownership.
Game concepts

Develop Narrative

Collaborative feedback

Levels and progress

Challenges

Master skills

Team achievements
Benefits of engagement – why gaming concepts work

Substantive input

Relevant plans

Crisis-ready personnel
But *where* do we start?
SHALL HE PLAY A GAME?

Gamification
Role playing games
Tabletop exercise (really just an RPG)
Where do RPGs fit?

Planning
- Business Continuity Plan
- Disaster Recovery Plan
- Incident Response Plan

Testing
- Coverage (breadth)
- Completeness (depth)

Training
- New plans or processes
- Currency
TESTING
I FIND YOUR LACK OF TESTS DISTURBING.
Effective training
A “good” RPG

- Rich character development that represents the player
- Compelling environment that is fundamental to the game
- Story line through which players must work together to achieve clear goals
- Skilled game master
  - Understands all aspects of the game
  - Leads players through challenges
  - Does not compromise game integrity
RPGs and planning

Assume a role (character)
- More than just “playing” a character
- Each player takes on the role of a character (i.e. “becomes”)

Understand the rules
- Must have core rules (start with policy)
- Should cover all foreseeable situations

Work with other characters to meet goals
- Encourage input
- Seek consensus
RPG benefits

Engagement

Team goal pursuit

Outcome ownership
Where to get guidance

- Look internally
- Explore on-line
- Engage external resources
Example IR planning scenario (phase 1)

- Split into groups
- Randomly assign each group a domain
  - Sample: https://www.sans.org/security-resources/policies
  - SANS example policy categories
    - General
    - Network Security
    - Server Security
    - Application Security
- Ask each group to create a list of incidents and response plans
- Have each group present a story based on findings
- Provide incentive for creative response
Example challenge scenario (phase 1)

- Small fire just outside the data center, setting off the alarm system
- Sprinkler extinguishes the fire by the time the fire department arrives
- The building has been evacuated
- Personnel and the media are aware of what happened
- Then, as people begin to go back inside
  - The receptionist takes a call from someone who indicates that the fire is "only the beginning" because the company hasn't treated him right
Readiness depends on testing. Want to play some more?
“It is better to be prepared than surprised”

- Dr. Michael Yousef
Ready  Set  Secure
Resources

- Dr. Michael Solomon (michael@solomonconsulting.com)
- NIST SP 800-34 “Contingency Guide for Information Technology Systems”
- ISO 17799 / COBIT
- Disaster response sample scenarios
- Business continuity tabletop exercises
- Gamemaster’s Guide to Incident Response
  - https://tisiphone.net/2015/07/13/gm-guide-to-ir/
- BCI online incident simulation game