SESSION ID: LAB1-R03

KEEPING YOUR CEO EMPLOYED AND YOUR BUSINESS IN BUSINESS

Mark Manglicmot
EY

Heather Gantt-Evans
EY
Trends in Cyber Exercises
Abstract

- As businesses become more digitally dependent, security ops become more intertwined with the business.

- To test, measure and validate this alignment, we suggest the use of cyclical, intensity increasing and threat scenario-driven war games designed to stress test the entire business' ability to respond.

- Today, cyber incidents are business incidents, cyber threats are business threats.
Introductions

- Around your table
  - Name
  - Where you're from
  - Organization
  - Role at organization
  - Favorite type of cheese?
Our approach

**Tell Me**
- Conversational “extended” tabletop exercise
- Bring your policies & procedures

**Show Me**
- Purple team exercise
- Blue team centric grading

**Prove It**
- Live war game
- Red team centric grading

Scenario Design with the Entire Business in Mind
Benefits

• **Cyclical** vs solitary
  • Ensures findings are implemented before the next exercise
  • Timely implementation and training of new processes

• Rooted in existing **processes and procedures**
  • Identify process failures within and across business functions

• **Business risk** vs cyber risk lens
  • Operations interact with other businesses functions regularly
  • Exercise scenario aligns to cyber and business risks
Exercise #1: Tell Me (Extended Tabletop)

- **Approximately 2-3 months** of planning
- **Approximately 4-6 hour exercise**, 2 hour debrief
  - Requires a single conference room
  - Series of injects (slides, calls, emails, videos, etc.)
- ** Entirely discussion based**
  - No technology or red team required
Exercise #1: Tell Me (Extended tabletop)

<table>
<thead>
<tr>
<th>Foundational Design Concepts</th>
<th>Standard Planning Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Business Wide</td>
<td>• Exercise objectives &amp; scenario design</td>
</tr>
<tr>
<td>• Threat Scenario Driven</td>
<td>• Participant selection</td>
</tr>
<tr>
<td>• Rooted in existing processes and procedures</td>
<td>• Threat scenario selection</td>
</tr>
<tr>
<td></td>
<td>• Red team attack diagram production</td>
</tr>
<tr>
<td></td>
<td>• Expected outcomes development</td>
</tr>
</tbody>
</table>
Exercise #1: Tell Me (Extended tabletop)

Once upon a time, a client wanted to design a tabletop exercise that...

- Was based on threat-centric and timely *scenario*
- Helped them meet *objectives*
- Highlighted integration gaps to a smart mix of *participants*
Exercise #1: Tell Me (Extended tabletop)

- **Threat scenario selection**: What does a threat scenario consist of?

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Capabilities</th>
<th>Intent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation State</td>
<td>Ransomware</td>
<td>Monetary Gain</td>
</tr>
<tr>
<td>Cyber Crime</td>
<td>Spearphishing</td>
<td>Brand Damage</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Lateral Movement</td>
<td>Access Relationships</td>
</tr>
<tr>
<td>Insider</td>
<td>Privilege Escalation</td>
<td>Theft of IP</td>
</tr>
</tbody>
</table>

*Example: Hacktivist DDoS of client-facing website servers to disrupt brand*
Exercise #1: Tell Me (Extended tabletop)

- **Attack diagram production**: How would the selected threat scenario unfold on existing architecture?
- Validate realism / accuracy
- Enable tabletop discussions and whiteboarding
  - Pinpoint point policies and procedures applicable
  - Track incident expansion
Exercise #1: Tell Me (Extended tabletop)

- **Expected outcomes development**: Do you know when and how the participants “should” respond?
  - Policy and procedure review
  - Exercise scenario design and timeline of events
  - Expected outcomes for each event
  - Grading scale
  - Lessons learned for process improvement
Group Participation Exercise I

**Time:** 15 minutes table prep, 10 minute debrief to the room

**Instructions:**
At each table, group together and leverage the following artifacts from President Business’ Worldwide Conglomerate (PBWC) to populate the provided risk register with ratings and determine PBWC’s highest risk threat scenario.

1. Business background and high value asset list
2. List of threat scenarios produced from a recent threat landscape assessment
3. Risk rating criteria
Exercise #2 Show Me (Purple team)

- Approximately **2-3 months** of planning
- **Full day exercise**, 2 hours debrief next day
  - Full participant awareness of specific start time
  - Red Team training before and after
- A mix of **tabletop discussion** and hands on the key-board **red and blue activity**
  - Requires a conference room and the Security Operation Center (SOC)
  - Pre-designed attack graph with planned red team pauses
  - Series of injects (slides, calls, emails, videos, etc.) and red team actions
## Additional Design Concepts

### Increasing intensity
- Key personnel “out of office”?  
- Out of bands comms?  
- Second shift?  
- Blocking allowed?  
- Advanced notice window?  
- Intelligence “clues”?  

### Blue team-centric grading
- Graders leverage “expected outcomes” to grade blue team

### Timely integration
- Is the security team keeping their business risk lens focused or just the cyber risk lens?  
- Expected outcomes need to include reaching out across the business
Group Participation Exercise II

**Time:** 15 minutes table prep, 10 minute debrief to the room

**Instructions:**
At each table, group together and leverage the provided red team attack diagram to:

1) Break the attack diagram up by pauses (i.e. what red-team actions will they take during their “turns” and when will they pause)
2) List expected blue team reactions to be observed in periods of red team pause
Exercise #3 Prove It (Live war game)

- Approximately **3-4 months** of planning
- Possible **multi-day exercise**, half day debrief next day
  - Limited to no participant awareness of specific start time
  - Red Team training before and after
  - Requires a different staffing model for grading
- **Pre-defined battlefield, flags and objectives** with red team pauses
  - Series of injects (slides, calls, emails, videos, etc.)
## Additional Design Concepts

<table>
<thead>
<tr>
<th>Stress test</th>
<th>Red team-centric grading</th>
<th>Validate improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Red team activity necessitates multi-shift (24 hour ops), multi-day incident response</td>
<td>• Identify a series of red team objectives and flag captures to be leveraged within a grading scale</td>
<td>• 2 prior opportunities to revise their processes and procedures</td>
</tr>
<tr>
<td>• Test across time zones and geographies</td>
<td></td>
<td>• Have those revisions been properly trained?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Do the revisions have the intended effect?</td>
</tr>
</tbody>
</table>
Group Participation Exercise III

**Time:** 15 minutes table prep, 10 minute debrief to the room

**Instructions:**
At each table, group together and leverage the Red Team’s list of objectives and flags to:

1) Brainstorm ways to group and quantify a Red Team centric grading scale (to be used for grading blue team’s defensive performance)
Take aways

- **Value of exercise program** vs ad-hoc
- Key strategies and considerations for **design**
- Hands on discovery of **actual artifacts**
- Less intimidating and more **tangible next steps**
THANK YOU!
Mark Manglicmots
Mark.Manglicmots@ey.com
Heather Gantt-Evans
Heather.Gantt@ey.com