How to Develop a Cyber Breach Exercise for your Organization
Agenda

• What if Your Defenses Fail?
  – 10 Reasons to Lose Sleep

• What a Cyber Exercise Is – and What it Isn’t
  – “Routine Emergency” Vs “Crisis Emergency” Vs “Emergent Crisis”

• Eight Critical Elements that Make a Cyber Exercise Work
  – When Everything Quits Working

• Cyber Breach Design Principles

• It’s Only a Matter of Time
What if Your Defenses Fail?
10 Reasons to Lose Sleep

1. Cyber attackers are leap-frogging defenses in ways companies lack insight to anticipate.
2. Attackers are moving faster, defenses are not always keeping up.
3. Type of malware used in mass attacks is increasing, and is more adaptable.
4. Attackers are streamlining and upgrading their techniques, while companies struggle to fight old tactics.

…but wait, there’s more.

Symantec, April 2015
10 Reasons to Lose Sleep

5. The cyber-attack surface is expanding: Dynamic workplace, highly mobile workforce, and workers’ expectations have blurred the concept of a network perimeter.

6. Attacks go deeper into the silicon.

7. Attacks are getting increasingly more difficult to detect.

8. Cyber threats are evolving, with many more hackers being able to join in and “play.”

...yup, still more.

McAfee, 2015
10 Reasons to Lose Sleep

9. Ransomware is now dominating the malware market.
   – It’s highly profitable.
   – Although not a new threat, it has evolved to become the most profitable malware type in history, and a growth industry.
   – Businesses are now becoming a target of choice.
   – Increasingly, it targets enterprise users.

...and one more.

Cisco Midyear Report 2016
10. Internet of Things (IoT)
“We need to accept that we will never eliminate all risk, that nothing is permanently safe. And even if we could, it would be far too expensive.”

McAfee Labs 2016
The “Bad Guys”

• Lots of options:
  – Nation states.
  – “Hacktivists.”
  – Organized crime.
  – Kids in the basement.
  – Anyone who buys a malware kit on the dark web.
  – Your employees:
    o May 2016 survey: One in 5 employees will sell their password for a measly $150.
What a Cyber Exercise Is – and What it Isn’t
It is NOT a Technology Exercise, *Per Se*

- Yes, technology is the underlying theme.
- However…
It’s About *Impact* to the Company

- This is very likely a situation that you have never *really* planned for.
  - What companies normally plan for are “*routine* emergencies.”
  - This is a “*crisis* emergency” or an “*emergent* crisis.”
“Routine Emergencies”

• "Routine" does not mean "easy."
  – "Routine" refers to the relative predictability of the situation that permits advanced preparation.

• It means you are able to take advantage of lessons learned from prior experience.

• You are likely to have thought about what to plan for and what is needed, and you have probably trained for it and done exercises for it.
“Crisis Emergencies”

- These are distinguished by significant elements of *novelty*:
  - Threats never encountered before.
  - A familiar event occurring at unprecedented speed.
  - A confluence of forces, which, while not new, in combination pose unique challenges.

- Because of the novelty, plans and behaviors that might work well in "routine" situations are frequently grossly inadequate in crisis emergencies, and might even be counterproductive.
Crisis Emergencies Require Different Capabilities

1. **Diagnose** the elements of the novelty.

2. **Improvise** response measures adequate to cope with the unanticipated aspects of the emergency.
   – Borne of necessity, these might be actions quite different than ever done before.

3. **Respond** in a creative way, and be extremely adaptable to execute improvised solutions.
Emergent Crises

• These pose special challenges in terms of recognizing novelty because they look much like “routine emergencies” in their early stages.
  – Only later do they reveal their unusual characteristics.

• Leaders may be slow to see the new features that require a different response. They become fixated on their original solution.
Eight Critical Elements that Make a Cyber Exercise Work
#1: Obtain Management Support

- You will discover things in a cyber exercise that will make people very, very uncomfortable.
  - You need to know that right up front.
- This is not a witch hunt, nor is it a blame game.
  - “We are open. We are looking for issues we have not thought about before, and thinking that needs to be refined.”
#2: Engage a Willing Technology Team

- This exercise is scary for an IT department. They are fearful that they will:
  - Be blamed.
  - Look bad.
  - Look like they could have or should have done more.
- You need them as your ally AND you need to provide them cover.
#3: Gather Two Strong Design Teams

• Technology Design Team:
  – The Technology Design Team develops the main cyber attack narrative.
  – Everything else nestles into this storyline.

• “Usual” Design Team (business units):
  – Key lines of business: Human resources, communications, facilities, security, and others as necessary to support the narrative.
#4: Focus on **Impact**

- Do that by using highly specific exercise injects.
- The Technology Design Team designs the cyber attack story.
  - This must be carefully thought out and translated so that the business unit team can work with the information.
- The Business Unit Design Team then uses the IT narrative to tell the business story through injects that describe the impact.
  - Remember: If you don’t tell them, they don’t know what’s happened.
#5: Conduct the Right Exercise Type

- The exercise must include a way to develop the story and allow the participants to experience the true impact:
  - Advanced tabletop.
  - Functional.
  - Full-scale.

- The common thread through these exercise types: They all use a Simulation Team.
#6: Expose The Perpetrator

• The story must leak out to the public.
  – In our exercises, we normally have the perpetrator revealed through social media.

• Because:
  – If it isn’t public, it becomes your little secret.
  – We want it out so the players have to deal with reputation and brand issues.
#7: Write a Well-Honed After-Action Report

- The AAR must have carefully constructed observations and recommendations.
  - Recommendations should be factual and tie to the exercise learnings.
  - Divide recommendations into likely sections: Cyber security, communications, business continuity, incident management, executive management, IT, others as appropriate to your company.
  - Even if there are a zillion learnings, be positive and upbeat ("You have formally identified the issues; that’s a big plus!").

- Know your political environment and write the AAR accordingly.
- Be careful of the word “recommendations.”
#8: Hold a Post-exercise Follow-Up

- This is the most impactful exercise we have done in our entire practice.
  - The AAR will likely be viewed by directors, executives, auditors, and others.
  - It will likely create a long list of action items that those noted above will want solutions for.
  - Share the cyber attack narrative with key decision-makers.
  - Strike while the iron is hot. They want to resolve these issues, and may put a high priority on funding.
When Everything Stops Working
When Everything Stops Working...

• Everyone will reach for their plans:
  – Business Continuity.
  – Crisis Communications.
  – Crisis Management.

• What type of answers will they find there for this situation?
  – Simple answer: “Not much!”
RTOs and RPOs

• Recovery Time Objective (RTO): How much *downtime* is tolerable?
• Recovery Point Objective (RPO): How much *data loss* is tolerable?
Out of Danger Comes Opportunity

Emergency Management & Safety Solutions
Data Loss

• Potential options:
  – Go back to your last “clean” back-up.
  – Use paper back-ups to fill in the gap.

• How do you do that?
You can simulate this with an Exercise (No, really.)
The Critical Question to Assist the Design

• Ask yourself “Why are we doing this exercise?”
• The answer to this simple question holds incredible value.
  – Discovering the answer is like peeling an onion.
• The answer will tell you:
  – Your exercise goal, scope, and objectives.
  – How to produce injects to achieve the desired effect.
  – How to keep you and the Design Teams on track.
• This exercise will engage all of your players, with the exception of Facilities, and possibly Physical Security.
Type of Exercise

• A cyber exercise performs best in one of three formats:
  – Advanced Tabletop.
  – Functional.
  – Full-scale.

• The common feature of these three types of exercises is the presence of a Simulation Team.
  – Regardless of the type of exercise, to be effective with this scenario, you need a Simulation Team.
Activity One

• Part One:
  – Answer the big question, “Why are we doing this?”
  – Determine the type of exercise.

• Part Two:
  – Share.
Cyber Breach Design Principles
The Exercise Focus Is On Impact

• An Crisis/Incident Management Team exercise is totally focused on the impact of the event.
  – This deep understanding drives the development of injects.
  – This is not a Technology/Information Security event, *per se*; however, the cyber attack event must be credible and well vetted.
A Word about the Breach

• The exercise designer doesn’t need to know how the security penetration occurred in gory detail.
  – Watering hole, malware introduced by thumb drive, employee clicked on a phishing email, spearfishing, software flaw, poor password, unattended device, employee sells their password, etc.
  – It doesn’t matter how.

• The team just needs to know if it’s possible to happen within your IT environment.

• Is it possible?
  – 99.99999%* of the time, yes!

*Not an actual statistic 😊
You Need Two Design Teams

• The Design teams work to assist you in narrative and inject development:
  1. Information Technology/Info Sec Team will design the IT narrative and IT injects.
  2. Other business unit participants will design all the other injects that “dance” with the IT narrative and injects.
IT/Info Sec Design Team

• The IT/Info Sec Design Team meets first and must completely detail the situation.
  – They must identify the failures in exquisite detail, noting the date and time of the IT meltdown.
    • *This step is critical.*
  – Discuss how it could happen (phishing, watering hole, flash drive insertion, etc.). The situation only needs to be possible.
  – The business unit design team will then use that information to develop injects that “tell the story” of what is happening to them as a result of the situation/breach.

• At a minimum, the IT/Info Sec design will take two meetings, with homework in between. It could take longer, depending on the complexity of the situation.
The Non-IT Design Team

• Team members should include those with:
  – Strong knowledge of the overall business.
  – A depth of knowledge in their area or department, such as:
    o Key business units.
    o Legal.
    o Regulatory.
    o Communications.
    o HR.
• You will likely need between 5 and 9 committed individuals.
Engaging the Non-IT Design Team

• This team will get engaged in the process:
  – After the goal, scope, and objectives are decided.
  – After the basic outline of the exercise narrative and plan have been fleshed out.
  – After the IT team has built the IT narrative.

• Design Team members can help to vet the narrative, but are not involved in establishing the narrative.

• This Design Team may also need 2 – 4 meetings, with homework in between, possibly more, depending on complexity.
Activity Two

• Part One:
  – Detail members (by title) for your IT design team.
  – Detail members (by title) for your Business Unit design team.

• Part Two:
  – Share.
Exercise Plan
Standard Exercise Plans

• Type.
• Scope.
• Goal.
• Agenda.
• Objectives.
• Communications.
• Evaluation.
• Participant instructions.

• Artificialities and Assumptions.
• Narrative/scenario.
• Communication directory.

Note: Today’s discussion will not cover the bullets in red.
Exercise Goal

• The goal is the defined purpose of the exercise, answering the question, “Why are we doing this?”
  – This should be a brief and clearly-stated aim of what you want the exercise to accomplish.
  – Along with the exercise objectives, the goal drives the exercise design and keeps you on track.
Goal Development

• The goal is developed by finding out what the key players want to get out of the exercise.

• Conduct short interviews with key players identified in the scope.
  – Incident Commander of the team.
  – Business unit managers.
  – Other key individuals.

• Example of a cyber breach goal:
  • “Assess the ability of the Incident Management Team to manage a major cyber-security breach.”
“Covert” Exercise Goal

• If the topic of the exercise is meant to be a surprise to the participants, you won’t be able to clearly state what you are designing, as you might commonly do.

• Instead, go covert (or more generic):
  – “Experience a systemic incident that impacts the company and all of its locations.”
  – “Assess the ability of the Crisis Management Team to manage a company-wide event.”
  – “Assess the emergency response aspects of the company plan and overall team readiness.”
Scope: Who and What are You Exercising?

• These questions go hand-in-hand. The answers determine scope of the exercise.

• Your participants could include all or part of:
  – Information Technology and Security.
  – Crisis/Incident Management.
  – Crisis Communications.
  – Business units.

• The usual focus is a Crisis/Incident Management Team (and often the Executives, too); that’s the theme of this discussion.
Objectives

• Most exercises have between 3 and 5 overall objectives for all participants.
  – There may be additional objectives for a specific team, a department, or location.
• Used to guide the design and to assess the outcome.
• Objectives should be clear and understandable.
  – Simple.
  – Concise.
  – Measurable (when possible).
  – Achievable.
  – Realistic and challenging.
Objective Examples

• Assess the ability of the team to evaluate the incident and escalate to the appropriate teams.
• Assess the communication and escalation triggers between the IAT, Information Security and Senior Management.
• Develop internal and external communications for all of the key identified stakeholders.
• Validate who has the authority to disconnect technology when there is a significant business impact.
## Agenda

<table>
<thead>
<tr>
<th>Activity</th>
<th>Time</th>
<th>Discussion Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>9:00 AM – 9:05 AM</td>
<td>Executive</td>
</tr>
<tr>
<td>Exercise One – Real time</td>
<td>9:05 AM – 10:00 AM</td>
<td>Exercise Facilitator</td>
</tr>
<tr>
<td>Exercise Two – “An hour later”</td>
<td>10:00 AM – 11:30 AM</td>
<td>Exercise Facilitator</td>
</tr>
<tr>
<td>→ Report to Executives.</td>
<td>11:20 AM</td>
<td>Incident Commander</td>
</tr>
<tr>
<td>Debrief</td>
<td>11:30 AM – 11:55 AM</td>
<td>Phelps</td>
</tr>
<tr>
<td>Next steps</td>
<td>11:55 AM – 12:00 PM</td>
<td>BCP Manager</td>
</tr>
</tbody>
</table>
Activity Three

• Part One:
  – Develop your goal.
  – Develop two objectives.
  – Determine the scope of the exercise.

• Part Two:
  – Share.
Where the rubber hits the road
Exercise Narrative

• The world is your oyster…there is lots to choose from. Our most commonly used narratives:
  – Malware…so much to choose from...
  – Ransomware…this past week….OMG!
  – DDoS
  – Jackpotting
Exercise Artificialities

• These are things that are not true but that exist to advance the purposes of the exercise:
  – Date and/or time of day change.
  – Equipment that is available or not available but is necessary to conduct the exercise.
  – Conditions in place necessary to conduct the exercise.

• Examples:
  – “The weather is hot and humid; temperatures will exceed 100 degrees.”
  – “John Smith is on vacation and is not available.”
  – “The employees whose last names begin with the letters B, G, M, and T are not available at all.”
  – “The date is <scenario date>.”
Developing Exercise Injects

• Injects continue the story that began with the baseline narrative.
  – The only way participants know something is different or has changed is by the *injection* of new information, hence “*injects*” (sometimes referred to as “*inputs*”).
  – Think of them as a continuation of a story, acts in a play, or chapters in a book.

• Most injects ultimately ask the recipient to **do something**.
  – Therefore, most injects will have one or more questions to be answered or issues to be resolved.

• They can also provide:
  – Additional background information for the storyline.
  – An “FYI” relating to an issue or situation.
Remember

• In a well-designed exercise, the players only know what you tell them.
Inject Components

• **Time:** When it will be delivered.
• **Caller name:** The source of the inject.
• **Mode:** The method of inject transmission.
• **Inject routing:** Person or team receiving the inject.
• **Content:** Text of the inject.
• **Notes:** “Acting tips” or other notes helpful to the delivery of the inject or the action expected to result from the inject.
# Inject Examples

## NOTES FOR THE SIMULATION TEAM:
- For the purpose of the exercise, it is Monday, August 8; it is the real time.
- A number of internal users have received ransomware threats on their desktops.

<table>
<thead>
<tr>
<th>Call #</th>
<th>Timing Notes</th>
<th>Route to:</th>
<th>Caller's name, title, and dept</th>
<th>Call Script</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2:00</td>
<td>&lt;&lt;Who gets it???&gt;</td>
<td>&lt;&lt;Caller’s name, title, and dept&gt;&gt;</td>
<td>Two of my sales staff here at the office, &lt;&lt;name&gt;&gt; and &lt;&lt;name&gt;&gt; both just told me that they got some kind of message on their screen demanding a million bucks in order to get their data back. Is this some type of prank? If so, it’s not funny!</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2:05</td>
<td>&lt;&lt;Who gets it???&gt;</td>
<td>&lt;&lt;Caller’s name, title, and dept&gt;&gt;</td>
<td>Chicago customers are swamping Tech Support because they are getting error messages. Error messages include “file not found,” “zero-bit file,” and “cannot read data.”</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2:08</td>
<td>&lt;&lt;Who gets it???&gt;</td>
<td>&lt;&lt;Caller’s name, title, and dept&gt;&gt;</td>
<td>We’re seeing lots of social media posts from our customers not being able to close or fund loans because you’re having some sort of data breach. What can you tell us? When will the problem be fixed?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2:11</td>
<td>&lt;&lt;Who gets it???&gt;</td>
<td>&lt;&lt;Caller’s name, title, and dept&gt;&gt;</td>
<td>Listen, this is pretty serious, isn’t it? Should we just pay the ransomware money so we can get our data back?</td>
<td></td>
</tr>
</tbody>
</table>
Inject Delivery Form for Advanced Tabletop
Exercise Realism

• If you have the budget, use A-V tools to deliver injects:
  – Inserts a sense of reality into the exercise.
  – Invites the participants further into world of make-believe.
  – Gives a better sense that something has *really* happened.
  – Gives the communications people something tangible to react to.

• AV options; mocked up versions of:
  – Radio broadcasts.
  – Press releases.
  – Emails, faxes, or other documents.
  – Video footage.
One Key Component

• It must be public.
• The hacker/perpetrator must expose you.
• This can be done many ways:
  – Hacker blog.
  – Video or info release to one or more news agencies.
  – Radio.
  – Social media, such as Twitter, YouTube, Facebook.
Make it Public Because…

• This creates a public reputation / brand issue.
  – Activates crisis communications in a big way.
  – Engages the executives at a new, deeper level.
  – Creates anxiety among employees.
  – Has the ability to engage and activate all key stakeholders.
Simulation Team

• Your best simulators were likely design team members.
• You need both an IT and Business Unit team.
• Characteristics of a good Simulation Team member:
  – Has a good overall knowledge of the company.
  – Has a good knowledge of specific departments that are being exercised.
  – Has a good attitude, good acting, team player, creative.
  – Is able to produce “credible scenarios” and yet stay on course with the exercise plan.
  – Hint: Design team members make great Sim Team members.
Sim Team Guidelines

• The Simulation Team can deliver:
  – Pre-scripted injects.
  – Corrective “on-the-fly” injects.

• They can keep the team, narrative, and exercise on track.

• A Simulator must:
  – Deliver the inject at the stated time.
  – React convincingly to the inject recipients’ comments.
  – Ensure that injects are kept active until they have been dealt with properly.
Activity Four

• Part One:
  – Identify if you need any artificialities. If so, outline them.
  – Develop a likely cyber narrative.

• Part Two:
  – Share.
It’s Only a Matter of Time
Get Going!

- Do research; peel back real events.
- Obtain buy-in to do a cyber exercise.
- Secure inside cyber assistance from IT (and provide them with lots of assurance).
- Develop the exercise plan, validate, and vet as necessary.
- Select a great exercise Design Team and sign them up to be Simulators.
- **What are you waiting for?**
Thank you

Regina Phelps
Emergency Management & Safety Solutions
San Francisco, California
@ReginaPhelps
Linkedin.com/in/reginaphelps
Regina@ems-solutionsinc.com
www.ems-solutionsinc.com