THE IMPORTANCE OF DESIGN TEAMS IN CREATING A TARGETED CYBER BREACH EXERCISE

BY REGINA PHELPS

Businesses and organizations defend against unending attempts to steal their computer data or damage their systems. Few, however, have serious plans for how they will respond to the impact of an actual breach. And even fewer stress-test those plans. Exercising a cyber-breach scenario forces real-time decision-making and actions. Creating an exercise with a cyber-incident scenario is infinitely more complicated than creating one with a "normal" emergency scenario, and requires special care in design.

Where to Begin?

Let's say you are tasked with creating a cyber-breach exercise. You're probably not quite sure how to go about it. What you need to make this exercise "spot on" is a highly-tailored narrative and highly-specific injects built around a set of pre-defined technology and information security incidents. You can't do that alone; you need help. And you don't need just any help, you need the right help. What you need are TWO Design Teams.

Why You Need Two Design Teams

You need two Design Teams because you need two very distinct and different sets of skills. First, you need a Technology Design Team that is very technical, detailed, and deeply in the weeds of the scenario. You should spend a lot of time picking the right narrative and then dissecting it. The Technology Design Team's main focus should be to identify all the different affected systems and their interdependencies and connection points.

You will also still need a Business Unit Design Team, but the Technology Design Team needs to do their work first, because you can't create the overall exercise injects until you know the technology issues and failures. Think of it like a Christmas tree

– the technology issues, failures, and problems are the trunk and branches; they provide the solid foundation for the story. The business unit injects are the reaction to those issues – like ornaments hanging on the tree. You can't hang the ornaments without the trunk and branches, and you can't design the business unit injects until you know the IT failures.

This author's firm, EMSS, always establishes the technology design first, followed by the business design. We then circle back with the technology team to review the business unit injects to make sure they align with the stated technology issues.

Technology Design Team

For a cyber-based scenario, there are often five to eight members on the Technology Design Team. (Because of their experience in the company, some members can cover multiple topics.) You'll likely need subject matter experts in the following areas:

- Information Security
- Infrastructure
- Application Development & Support
- Network
- Database
- Network Operations Center
- Help Desk
- Storage

Business Unit Design Team

Your Business Unit Design Team has one primary goal – to develop the exercise injects that play off the cyber-breach story, see Table 1. (As mentioned, the Business Unit Design Team shouldn't hold meetings until the Technology Design Team has completed its work.) The type of members needed for your Business Unit team will depend on the overall cyber-breach narrative. If you have a physical impact in the story as well as a cyber impact, you will also need to include facilities and security on your Business Unit team.

A top-notch Business Unit Design Team member will have several qualities; they should have:

- A good basic knowledge of the overall business.
- At least a year or more with the company in order to know some of the ins and outs of the place.
- Subject matter expertise in an area you will likely be touching on in the narrative.

> "If everyone is moving forward together, then success takes care of itself."
>
> – Henry Ford

A typical Design Team will include members from the following departments:

- Representatives from all of the key lines of business (to help you develop highly specific business injects).
- Facilities.

CONTINUED ON PAGE 20

Call #	Time	Design Team Member (Simulator)	Routing	Caller's name, title, dept	Call Script
1				←Caller name, title, dept→	We have issues printing ←name of→ reports. Sometimes it prints and other times it does not. Can someone help us?
2				←Caller name, title, dept→	We posted our transactions into the Billing system, however the data did not transfer to SAP, therefore, we can't balance our end-of-day.
3				←Caller name, title, dept→	We try to insert the ←name of→ reports into Sharepoint but cannot because we are unable to access ←app name→. Is there an issue with Sharepoint?
4				←Caller name, title, dept→	I cannot open the ←name of→ spreadsheet. I can't update my cash flows.
5				←Caller name, title, dept→	My workstation was identified as one of the ones that are compromised. Do I have to use another workstation? Where can I go to work?

Table 1, Sample Injects

CONTINUED FROM PAGE 19

- Physical Security.
- Human Resources.
- Communications.
- Investor Relations.

Note that the departments listed above are typical of Design Teams. Your organization may benefit from having team members representing a different 'slice' of your business.

The "Other" Role for Your Design Team Members to Play

Design Team members usually make great Simulation Team members. Because they have been involved in exercise design and inject creation, they know the exercise intimately and are already a cohesive team. (They can help on the Simulation Team, but would not be players in the exercise because of their knowledge of the injects. The author's book reviews this in greater detail. See below for a link to the book.) If you plan to ask them to be Simulators in addition to their design job, in the interest of fair disclosure regarding the time commitment for the project, be sure to include that task when you ask for their participation at the beginning of the process. Besides the time commitment needed as a Business Unit Design Team member (see next section), here is the additional time your Designer-turned-Simulator needs to carve out (times are approximate):

- Simulation Team orientation: Ninety minutes to two hours (usually occurring a few days before the exercise).
- Exercise day: However long you have scheduled the exercise.

> "Alone we can do so little, together we can do so much."
>
> – Helen Keller

Design Team Meetings

In our experience, most Design Team meetings last between 90 minutes and two hours. They work equally well when held face-to-face or as a conference call. However, you might wish to do the first meeting face-to-face to make sure everyone is on point. EMSS routinely holds Design Team meetings by conference call, and find them to be a highly efficient and effective use of everyone's time.

How Many Meetings and How Often to Have Them

For an "average" cyber exercise, EMSS usually holds around four meetings with each team, for a total of eight meetings (four technology, four business). However, for a large Functional or Full-scale exercise, it's entirely possible to need between six and eight meetings for each team. It all depends on the scenario complexity, the length of the exercise, the sophistication of the team, and the team's familiarity with the exercise design process itself.

Design Team meetings are usually held every other week. You don't want to lose the team's momentum by waiting too long between meetings. Conversely, the team needs time to do their homework (e.g., doing their 'trench coat' research or writing injects).

Who Does What?

The Technology Design Team has two major tasks: To develop the cyber-breach narrative, and to develop the cyber-breach injects. The Business Unit team develops the injects that reflect the impact of the technology situation on the business side of the organization. (And, as mentioned before, hopefully, both sets of team members will act as Simulators on the day of the exercise.)

Summary

Both Design Teams are critical to a successful cyber exercise. Selecting the right team members will make your exercise credible, exact, and challenging. It will also engage more people in your program and help to build a culture of awareness and support for your program.

This author's book, "Emergency Management Exercises: From Response to Recovery, Everything You Need to Know to Design a Great Exercise" focuses on Advanced Tabletop, Functional, and Full-scale exercises, and covers everything from broad strategies to minute-to-minute decision-making. It also provides very specific, step-by-step instructions – starting from the earliest planning to after-action reports. Find it on Amazon at http://tinyurl.com/j6skbh8.

ABOUT THE AUTHOR

Regina Phelps is an internationally recognized expert in the field of crisis management and contingency planning. She is the founder of Emergency Management & Safety Solutions (EMSS), founded in 1982. Services include crisis management team development, pandemic planning, exercise design and facilitation, and business continuity plan development and audits. She can be reached at: Regina@ems-solutionsinc.com and www.ems-solutionsinc.com.