everbridge®

6 Keys to Developing a **Cyber Attack Training Exercise**

by **Regina Phelps, CEM, RN, BSN, MPA – Principal, EMS Solutions Inc.**

WWW.EVERBRIDGE.COM

6 Keys to Developing a Cyber Attack Training Exercise

Introduction

It seems there isn't a day that goes by without another story of a cyber attack or breach. It has almost become a "breach a day"! Not only is there confidential company or customer information exposure to worry about, these events are expensive on many levels: Detection of the problem in the first place, recovery of data, the loss of information, and disruption to the business, among other things. And, of course, this does not take into account the damage to a company's reputation and loss of current and future business. The Ponemon Institute found the average annual cost of responding to cyber attacks was $12.7 million, up 96 percent over the previous five years.[1]

Companies are spending millions of dollars to prevent these attacks from occurring, which is a wise and prudent investment. Few, however, is talking about how to deal with the impact of such a breach. We have surveyed our clients, professional colleagues, and firms and found no one is planning for the impact.

We have done numerous real world cyber attack exercises to train organizations on mitigating the impact of a cyber breach and have found them to be the most effective and rich narratives we have ever used in over thirty years of practice. Do you want to get your executives and incident management team ready for such a cyber attack? Then you need to do a cyber attack training exercise.

What Makes Cyber Attack Training Exercises So Different?

One of the things I often hear continuity professionals say is that they "plan for the worse-case scenario." Whenever I hear that come out of someone's mouth, I immediately stop them; this is simply not true. We don't plan for the worse-case scenario, we plan for what we think will happen, what is called a "routine" emergency. What we plan for may be a really bad situation, but there is not enough time, money, or risk appetite to plan for the truly worse-case scenario.

---

[1] Cost of Cyber Attacks Jumps for US Firms: Study, Security Week, October 2014 http://www.securityweek.com/cost-cyber-attacks-jumps-us-firms-study

“Routine” Emergency

To be clear, routine emergency[2] does not mean "easy." A routine emergency can still be difficult and challenging. In this context, “routine” refers to the relative predictability of the situation that permits advanced preparation. This risk is in our risk profile and we likely have been able to take advantage of lessons learned from prior experiences. You are likely to have thought about what to plan for and what is needed, and you have probably trained for them and done exercises for them. Our incident management, crisis communications, business continuity, and disaster recovery plans are filled with strategies to manage routine emergencies.

“Crisis” Emergency

A crisis emergency[3] is a much different animal. These types of events are distinguished by significant elements of ***novelty***. This novelty makes the problem much more difficult to diagnosis and then deal with. This type of emergency can have the following characteristics:

- The threats have never been encountered before, therefore there are no plans to manage it.
- It may be a familiar event, however, it is occurring at unprecedented speed and therefore developing an appropriate response is severely challenging.
- There may be a confluence of forces, which, while not new individually, in combination, pose unique challenges to the response.

The novel nature of a crisis emergency becomes a game-changer. Our plans, processes, training, and exercises that may work well in routine emergency situations are frequently grossly inadequate in a crisis emergency, and may even be counterproductive. We realize that we have to start from scratch.

The crisis emergency also requires different capabilities; in other words, the plans and behaviors we use for routine emergencies just won’t work. The first thing we must do is to *identify* the elements of the novelty; we must determine what makes this situation so different from others. In a cyber attack or breach, this novelty can often surprise us. We might begin the process thinking it is one thing, and then over time, we realize it turned out to be something quite different. For example, we may think we are dealing with a routine IT problem or outage, and then over time, we see it is something more significant and sinister.

---

[2] Managing Crisis: Responses to Large-Scale Emergencies, Arnold Howitt and Herman Leonard, CQ Press, page 5

[3] Ibid, page 6.

Once we have identified the real problem and understand that our routine plans won't work, we have to improvise response measures that will be suitable to cope with the unanticipated aspects of the incident. In other words, we are in new territory; this hasn't been done before. Created out of necessity, these responses may be actions quite different than ever done before. Handling a crisis emergency may feel like you're *building* an *airplane while flying it at the same time. It's not pretty, but it may be necessary.*

Lastly, in a crisis emergency, we must respond in creative ways and, *at the same time*, be extremely adaptable as we execute these new and improvised solutions. We have to be on "full alert" at all times, as we don't know how the situation will change, and we must be prepared to shift or dart at a moment's notice. All of this makes people quite anxious, and during an exercise, this anxiety often manifests itself in varying degrees of excessively loud voices or hushed voices, frantic activities, and nervous laughter.

Six Keys to Developing and Managing a Cyber Attack Training Exercise

To manage this very different type of exercise, you need to have six things in place to make it work:

1. Management Support

Right off the bat, senior management needs to understand that a cyber attack training exercise is likely to produce many learnings and issues that will need to be resolved, and it will present topics that they have never thought about or deeply understood. This could easily make people feel uncomfortable with quite a few unanswered questions at the end of the experience. As you explore the topic, you will also likely need to provide some cover to the IT and Information Security departments so that it doesn't become a blame game or a witch hunt.

2. A Willing IT Department

IT needs to be an active planner in the exercise. You need several excellent IT staff members who will not be players in the exercise to be part of the design process. You need them to help you determine what the cause will be. When you first begin, this will undoubtedly make them uncomfortable, because in the back of their mind, they are going to be fearful of being blamed. You'll need to reassure them that's not the goal of the exercise.

The first question you need to ask the IT department is, “Could we be hacked?” The answer will inevitably be “yes.” The next question is, “How could that happen?” The list is long but could include things such as phishing, watering holes, or infected flash drives. You just need to find a likely means, not a deep exploration of the intrusion. You need the IT team as your ally and you may need to provide them some cover.

3. Two Design Teams

You need two design teams: An IT/Information Security design team, and a standard Exercise Design team. The IT/Info Sec team needs to do a deep dive on the narrative and develop the timeline of issues that happened before the exercise’s scenario date, and then provide a very detailed timeline of what happens during the exercise. Once they have developed the breach timeline, the other design team can begin to develop their injects.

The standard Design Team should include key lines of business, Human Resources, Communications, Facilities, Security, and any other key departments. Those team members should take the IT narrative and timeline, and develop their injects, which will tell the story of the IT problems from their perspective. Remember: In an exercise, if you don’t tell the players what’s happening, they don’t know what’s going on and will invent things. The injects are the way we tell them the story.

4. The Right Exercise Type

There are three styles of exercises that can be used with a cyber narrative: Advanced Tabletop, Functional, or Full Scale[4]. What they have in common is a Simulation Team. This exercise requires a Simulation Team to make it work. The teams going through the experience need to have someone to speak to as they work through the problems. If you don’t have a Simulation Team, you will not be able to work through the issues to a deep-enough level to gain value from the experience.

[4] Emergency Management Exercises, Regina Phelps, Chandi Media, http://tinyurl.com/pyt9p8x

5. Interwoven Narrative and Injects

The narrative for this exercise will have lots of nooks and crannies. It has a certainly complexity that can't be avoided. The story progresses through the injects, and the injects must "dance" with the IT narrative. The exercise players have to tease the information apart, work with the Simulators to figure out what's going on, and then improvise a plan. When they develop that plan, then the Simulators have to adapt to the new plan and, in some cases, create injects "on the fly" to make it all work. The narrative and the injects are constantly ebbing and flowing together to tell the entire story.

6. Make it Public

One of the key aspects of this narrative is the potential damage to the reputation of the company. To damage that reputation, we have to "out" the narrative. We usually do this early on in the exercise by having our "perpetrator" post the story on a social media platform such as Twitter. (***NOTE***: Of course, we don't put a real post on Twitter. This is all done via "exercise magic.") We often have our AV team produce videos in a similar style as a hacker video, such as those done by Anonymous[5]. In exercises we have done, we play such a video for the participants, and watch as their jaws literally drop.

To make it even more interesting, we then create a second video by one of the local news stations, saying they are sending reporters to the company under siege seeking official comments and interviews with executives. Mission accomplished! Company outed! The players then have to deal with the fallout.

Communication Challenges

On first glance, you may not think this exercise presents unique communication challenges. Think again! There are many actions that are likely to occur in such an exercise that will severely challenge communications. In addition to 'standard' communications issues of putting out press releases and social media posts addressing the issue in general, bigger problems occur if the decision is made to cut the company's internet connection. In even more severe cases, the decision may be made to cut the core network. If connectivity is cut, here are some of the communication challenges you might face:

[5] Anonymous YouTube channel https://www.youtube.com/user/AnonymousWorldvoce

- If your phone and voice mail system is VOIP-based, you may lose your company phone system, severely hampering communication.
- If your employee hotline runs through your voice system, this could be lost.
- If your company website is hosted in-house, it may go down, meaning your customers, employees the general public, and the media can't find you. (If it's hosted by a third party who hasn't been affected by the breach, you may not have this problem.)
- If company telephone bridges are running through your phone network, they may not be available.
- If you bring down the core network, every computer becomes a standalone machine with no access to your company's records. Your human resource information, employee contact information, vendor lists, or other key phone lists may be inaccessible.

How will you communicate? Once this breach is public and everyone knows, your need to be available, communicating, and visually managing the situation is critical. Our clients with third-party or outsourced emergency notification systems (ENS) were ahead of the game. The big plus for them is being able to use their ENS for the following activities:

- Employee information: Pushing information to employees about the company status, and providing talking points and other key pieces of information.
- Conference bridges: Using toll-free conference bridges for employee, vendor, senior management, Board of Directors, and other key stakeholder phone calls.
- Stakeholder groups: Using pre-defined groups that had been created for all of their key stakeholders to push information via phone, text or email.

If you don't currently use an ENS or IT incident notification system, this may be one of the key learnings in the exercise. If you have an ENS but only use it for a limited set of contacts (i.e., your employees), you will quickly discover that there is a lot more that it can be used for which makes good business sense. Get the most out of your money by using your ENS for as many things as make sense.

Going Forward

For businesses, the risk of experiencing a data breach is higher than ever with almost half of organizations suffering at least one security incident in the last 12 months.[6] The C-suite and Board members can no longer ignore the drastic impact a data breach has on company reputation. Meanwhile, consumers are demanding more communication and remedies from businesses after a data breach occurs.

If the future is anything like the past, cyber incidents in our company's lives are not going away anytime soon. Life will continue to be complicated. Plan your next exercise to be a cyber exercise. Focus it on the impact of a breach and how your company will deal with it. And based on the probability of a cyber event, you had better get going!

[6] Data Breach and Industry Forecast 2015, Experian http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf

About Everbridge

Everbridge provides a unified critical communication suite that helps clients be better prepared, make better decisions, and respond quickly and confidently during disruptive events. When an incident happens, whether it's a natural disaster or an IT service outage, we automate communications to ensure that the right messages get to the right people at the right time.

Widely recognized by analysts as the market leader, Everbridge solutions are trusted by clients in all major industries and government sectors to connect with over 50 million people around the world.

THE ONLY END-TO-END PLATFORM

- **Planning**: Everbridge is easy to set up, maintain, and organize, meaning that you're always ready for a quick, coordinated response. Everbridge ensures that the right messages get to the right people - with the most advanced opt-in portal on the market, streamlined integration with internal and external data sources, and simple group and contact management.

- **Assessment**: When trouble strikes, you need rich insight, presented simply - so you can quickly assess potential impact and make an informed decision to avoid loss. Everbridge offers the only solution on the market that meets these demanding requirements, with the most advanced interactive dashboard in the industry.

- **Response**: In critical situations, ease-of-use can mean the difference between an effective response and a mistake that carries serious consequences. Everbridge is engineered to be simple to use under pressure, with a user interface that accelerates time-to-message and reduces the likelihood of errors.

- **Delivery**: Even during large-scale disruptions, Everbridge stays on. The most advanced platform in the industry ensures that you reach your contacts - every time. And with worldwide coverage and capabilities, including globally local calling infrastructure and data storage, we're ready to support you wherever your people are in the world.

Visit www.everbridge.com to learn more.