



1



Could It Happen to You? Absolutely!

- What are your chances of being attacked?
- 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
- You Can Simulate this With an Exercise
- Is there a solution to combat “nothing?”
 - Manual Workarounds in Three Steps
- It's Only a Matter of Time

2

Your Chances Are Really Good!

*“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:
 - Organized crime
 - Nation states
 - “Hacktivists”
 - Kids in the basement
 - Your employees – the Insider Threat
 - One in 5 employees will sell their password for a measly \$150 (reported in *Fortune Magazine*, March 30, 2016)







What a Cyber Exercise Is – and What it Isn't



www.ems-solutionsinc.com

5

5



It is NOT a Technology Exercise, *Per Se*

- Yes, technology is the underlying theme
- However...

March 2020

www.ems-solutionsinc.com

6

6



It's About *Impact* to the Company

- This is very likely a situation for which you have never *really* planned
 - 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
 - Born of necessity, these might be actions quite different than ever taken before
3. **Respond** in a creative way, and be extremely adaptable to execute improvised solutions



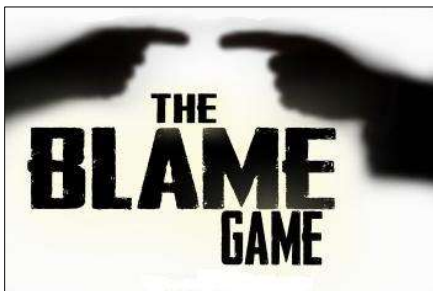
Emergent Crises

- 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
 - You must be open. You are looking for issues that you may not have thought about before or solved

#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

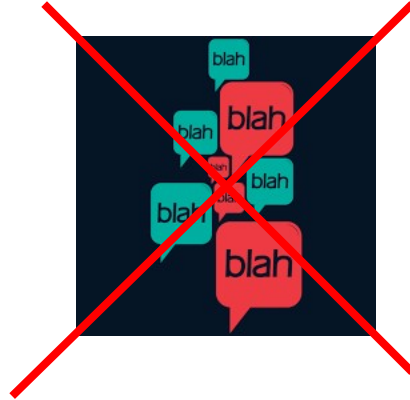


#4: Focus on *Impact*

- 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

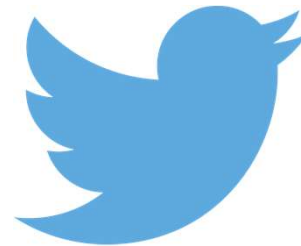
#5: Conduct the Right Exercise Type

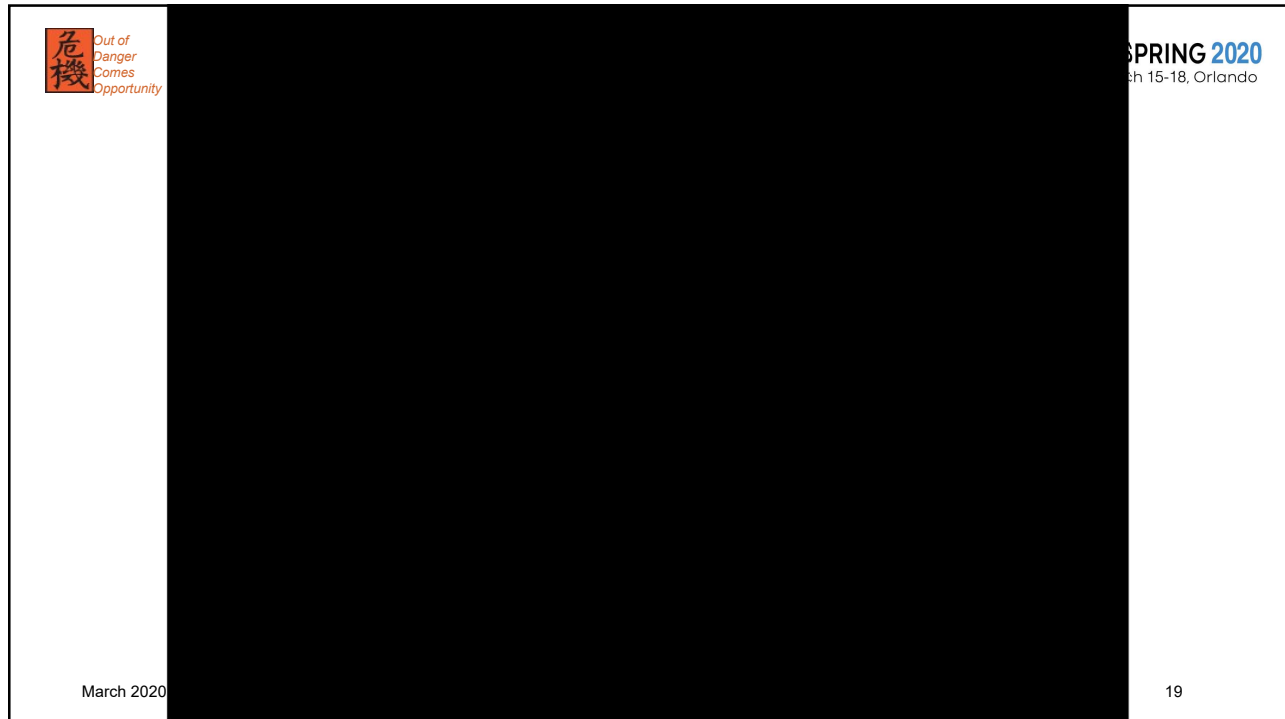
- The exercise must include a way to develop the story and allow the participants to experience the true impact:
 - Advanced tabletop
 - Functional
 - Full-scale
- The common thread through these exercise types: They all use a Simulation Team





#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





19



March 15-18, Orlando

#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, crisis 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”

March 2020

www.ems-solutionsinc.com

20

20



#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 for which those noted above will want solutions
 - 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...

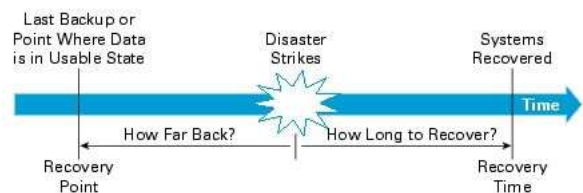


- Everyone will reach for their plans:
 - Business continuity
 - Disaster recovery
 - Crisis communications
- What type of answers will they find there for this situation?
 - One word...nothing
- This will then make everyone want to rethink:
 - RTO's and RPO's
 - Downtime
 - Loss of data



RTOs and RPOs

- Do we really ever think that we will have to live with our RTO's or RPO's? Really???
- Recovery Point Objective (RPO): How much *data loss* is tolerable?
- Recovery Time Objective (RTO): How much *downtime* is tolerable?



Downtime

- Go to your recovery time objectives:
 - What if you really had to live with downtime?
 - What if the downtime was longer?
 - What if it was *much, much, much* longer?



Data Loss



- Data loss is a real possibility. Potential options:
 - Go back to your last “clean” back-up.
 - Use paper back-ups to fill in the gap.
- How would you do that?

27





Four Audiences – Four Exercises

- Audiences
 - Business Units
 - Technology Team (Incident Response Team)
 - Crisis Management teams (tactical)
 - Executive Crisis Management teams (strategic)
- Key part of a well-designed cyber exercise?
 - Leave them in misery...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



A Word about the Narrative

- The exercise designer doesn't need to know exactly how the security penetration occurred
 - Watering hole, malware introduced by thumb drive, employee clicked on a phishing email, software flaw, poor password, unattended device, 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 ☺



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



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 Crisis Management Team to manage a major cyber-security breach”



Exercise Artificialities

- These are things that are not true but 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



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.

Call #	Timing Notes	Route to:	Caller's name, title, and dept	Call Script	Notes
START OF EXERCISE INJECTS					
1	2:00	<<Who gets it??>>	<< Caller's name, title, and dept>>	Two of my sales staff here at the office, <<name>> and <<name>> 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!	
2	2:05	<<Who gets it??>>	<< Caller's name, title, and dept>>	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."	
3	2:08	<<Who gets it??>>	<< Caller's name, title, and dept>>	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?	
4	2:11	<<Who gets it??>>	<< Caller's name, title, and dept>>	Listen, this is pretty serious, isn't it? Should we just pay the ransomware money so we can get our data back?	

Remember

- In a well-designed exercise, the players *only know what you tell them*



One Key Component

- If you are concerned about reputation and brand, 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



Exercise Realism

- If you have the budget, use A-V tools to deliver injects because it:
 - Inserts a sense of reality into the exercise
 - Invites the participants further into the world of make-believe
 - Gives a better sense that something has *really* happened
 - Gives the communications people something tangible to react to
- A-V options; mocked up versions of:
 - Radio and television broadcasts
 - Press releases
 - Emails, faxes, or other documents.
 - Video footage



Yes...Manual Work-arounds

- What does manual work-around mean?
 - *The ability to adequately perform an action/process through non-conventional means*
 - *For business, “non-conventional” means without the use of the internet, your core network or data held in your systems*
- Critical departments are severely challenged to continue critical operations without the access to the internet, core network or data



Questions to Consider

- Do your current plans have any manual work-arounds for this type of situation?
- What types of actions/work could a critical department do manually without access to the network?
- If a critical department had a bit of time to download something to help them do their job, what would that be?
- What does a critical department need to do to be prepared for this type of situation?



Business Units: Start With a Slow Meltdown

- And then have each team/department dig in and begin to explore:
 - Once the systems are completely unavailable for an “unknown” amount of time, have facilitators in each team pose questions and begin the discussion and take a deep dive
- When you ask them what can be done manually, most will say...nothing....
 - You will need to work with them to open their minds up to the possibilities
- The goal is to begin to explore what could be done with no or limited information
- Have an observer embedded with each team to capture key learnings
- Take the observations as a starting place and work through and create processes



Business Units: Sample Discussion Questions

- Does your current plan have any manual work-arounds for this type of situation?
- Before complete automation, how was work accomplished?
- What types of actions/work could your department do manually without access to the network?
- If you could have a bit of time to download something to help you do your job, what would that be?
- Given the widespread extent of the breach, what are the implications for your department? What could happen?
- What does your department need to do to be prepared for this type of situation?



Manual Work-arounds in Three Steps





Step One: Identify Impact to Critical Processes

- Assess the impact to business processes through workshops/training with each department
 - Use narratives (no internet / no network/loss of systems) to enhance their understanding of process implications
 - Identify and consider two-way dependencies in their processes – “upstream” and “downstream”
 - “What do I have now? What do I need to function?”



How to Document Manual Work-arounds

1. Identify the **impact** to critical business processes from not having internet or network access (or whatever the “thing” is your organization assumes will always be in place)
2. Unravel the business logic and automation behind the process to understand your needs
3. Encourage creativity and strike a balance between what’s optimal and what’s practical



Step Two: Unravel the Existing Automation

- Use scenarios (no internet / no network) to streamline the effort of developing manual work-arounds
- Ask contextual questions to ensure your work-around is robust
 - Timing of outage (end of day, mid-day, certain critical days of the month)
 - Duration of outage (a few hours, 24 hours, 48 hours, longer)
- Document this information in business continuity plans
 - “What do I need to have in place to perform this mission critical task?”



Step Three: Be Creative – Think Outside the Box!

- Business departments need to think creatively. How? Ask probing questions – in other words, dig! How was it done just a few years ago without much technology?
 - Confidentiality, Integrity and Availability
 - Minimum requirements
 - Downstream flexibility
- Be Realistic
 - “How else can I achieve this?”



Feedback from Other Clients

- “We’re accountants...get a pen and paper! Spreadsheets the old-fashioned way!”
- “We developed an *economist survival kit* with key files and software to ensure critical process could be completed”
- “We can walk to a Starbucks and jump on their WiFi”
- “We can blow the dust off the secure fax to send and receive that information”
- “We can reach out to trusted partners to provide that information”



Human Resources: A Simple Example

A critical process for Human Resources is payroll

- Scenario – loss of internet, network, access to any data
- Impact to process – impedes ability to process payroll
- Manual process
 - What do I have?
 - Isolated computer and a USB
 - What do I need?
 - Alternative means to connect with service provider
 - Back-up files saved to an encrypted USB



Finance Settlement: A Simple Example

A critical process for Central Banks is to be able to "settle" the books

- Scenario – loss of internet, network, access to any data
- Impact to process – unable to settle
- Manual process
 - What do I have?
 - Hourly transfers of critical information offsite in encrypted files
 - What do I need?
 - Isolated laptop and hotspot to access the internet
 - Back-up files saved to an encrypted USB



Immediate Benefits

- Greater awareness of business processes and confidence in the ability to deliver core services
 - Business identifies what is really important
 - Heightened awareness of processes crossing multiple business lines
 - Will make your business continuity plans much better and actionable
- Reduce overall risk and create a stronger resilience posture
- Remember to provide encouragement, reminders and celebrate the achievements



57



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?**

58



Thank you

Regina Phelps

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