

#IAEM2017

**Cyber Breach:
What If Your
Defenses Fail?
Design Exercises to
Map Strategy**



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 Stops Working
- You Can Simulate This with an Exercise
- It's Only a Matter of Time

A person wearing a dark hoodie is centered in the frame, holding a light-colored rectangular sign. The sign contains the text "What if Your Defenses Fail?". The background is a dark green world map with vertical columns of binary code (0s and 1s) overlaid. Several words are written vertically in a light green, monospace font: "PHISHING" on the far left, "INTRUDER" on the left side, "FRAUD" in the upper middle, "SURE" on the right side, "SPY" on the far right, "SERVER" on the left side, "KEY" on the right side, and "PASSWORD" on the far right.

What if Your Defenses Fail?

10 Reasons to Lose Sleep

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

...but wait, there's more.

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."

10 Reasons to Lose Sleep

9. Ransomware is now dominating the malware market.
 - Why? It is 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 targeting enterprise users.
 - Ransomware attacks in June and July have cost companies and governments millions of dollars. This is likely to continue and expand.



10. Internet of Things (IoT)

++
Average
--

Relative IPv4 utilization observed using ICMP Ping requests

Source: Carna Botnet

□

*“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

Who Are The Bad Guys?

- Lots of options:
 - Nation states.
 - “Hacktivism.”
 - Organized crime.
 - Kids in the basement.
 - Your employees:
 - March 2016 survey: One in 5 employees will sell their password for a measly \$150.



A person wearing a dark blue hoodie is sitting at a laptop. The person's face is obscured by the hood, and the background is dark with various white digital symbols like arrows, brackets, and letters floating around. The laptop screen is white and displays the title text.

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.

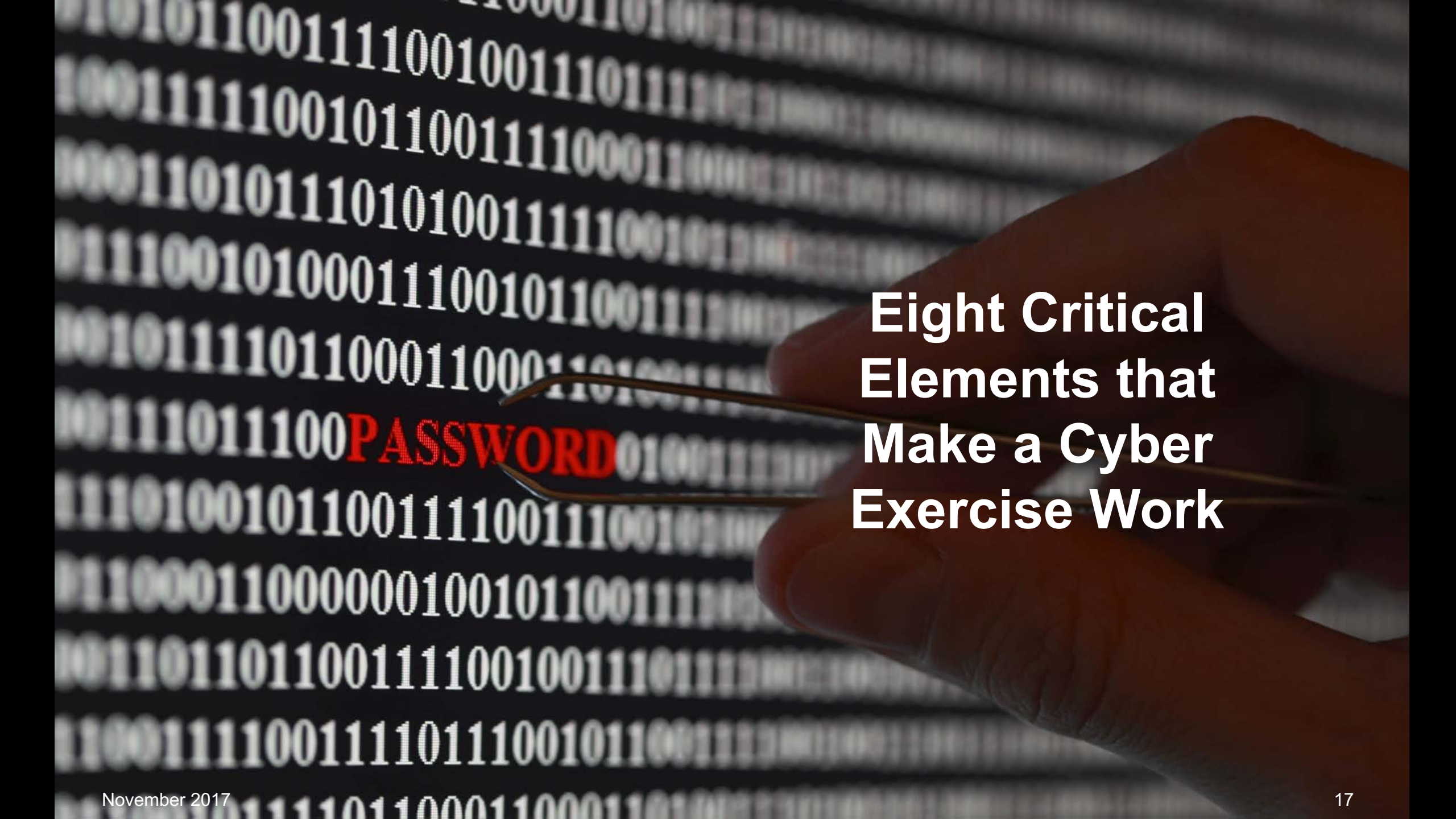
Crisis Emergencies Require Different Capabilities

- 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 “wed” to their original solution.



A hand holding a needle is positioned over a background of binary code (0s and 1s). The word "PASSWORD" is written in red, bold, uppercase letters across the middle of the binary stream. The overall image has a dark, moody aesthetic with a focus on digital security and cyber threats.

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

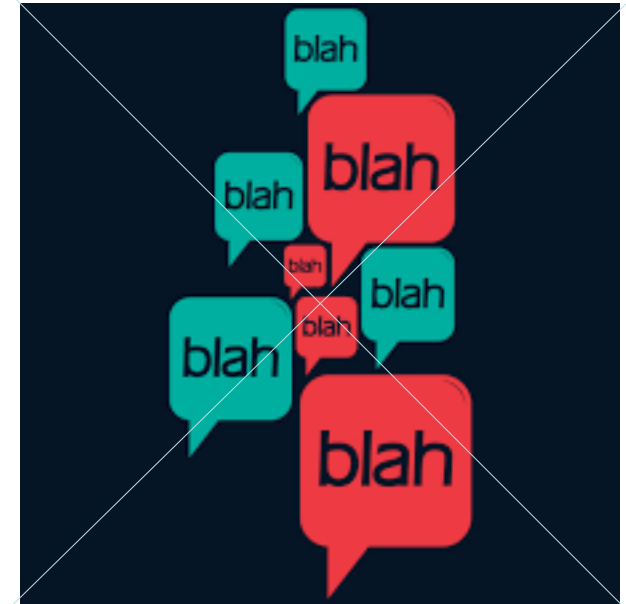
- Technology Design Team:
 - The IT Design Team develops the main IT narrative.
 - Everything else nestles into this storyline.
- “Usual” Design Team (business units):
 - Key lines of business: Human resources, communications, facilities, security, and others as necessary to support the narrative.

#4: Focus on *Impact*

- You do that by using highly-specific exercise injects.
- The IT Design Team designs the IT 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: Because it isn't real, if you don't tell them, they don't know what's happened.

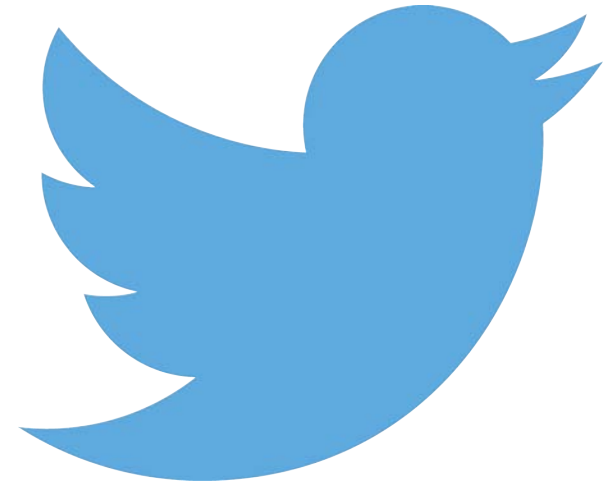
#5: Conduct the Right Exercise Type

- 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: “Out The Perpetrator”

- The story must leak out to the public.
 - In our exercises, we normally have the “perpetrator” being outed through social media.
- Why?
 - If it isn’t public, then 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 executives, Boards, auditors, and others.
 - It will likely create a long list of action items that those noted above will want solutions for.
 - Share the IT narrative with key decision-makers.
 - Strike while the iron is hot. They want to resolve these issues, and funding may become more available for this than anything else.

When Everything Stops Working

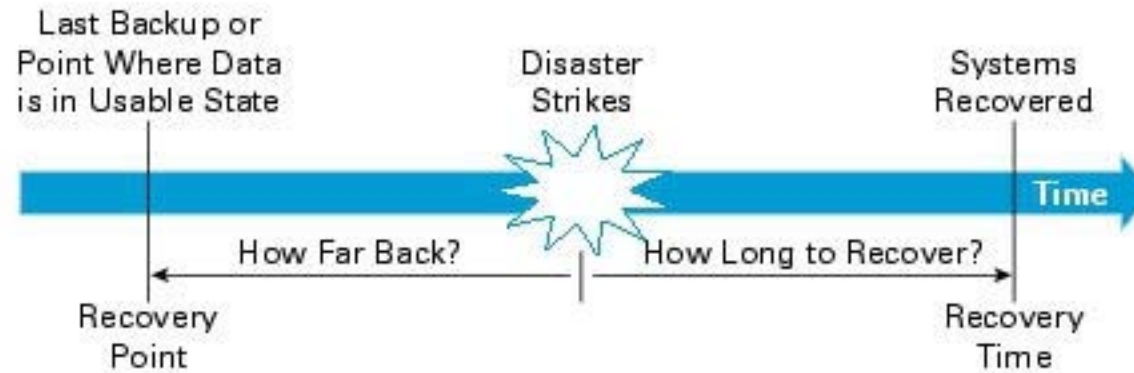


When Everything Stops Working...



- Everyone will reach for their plans:
 - Business Continuity or COOP plan.
 - 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?

MISSING

01010101110110100110100101001110010010001010101
1010101000101111001010010101011010100101001010
111010110111100101010101010101010011100111011000
0111011010110101110111010010011101110111010111001
0000011110101101011011111100000001001010100010

Lost Data :(

*** Last seen before major security breach! ***

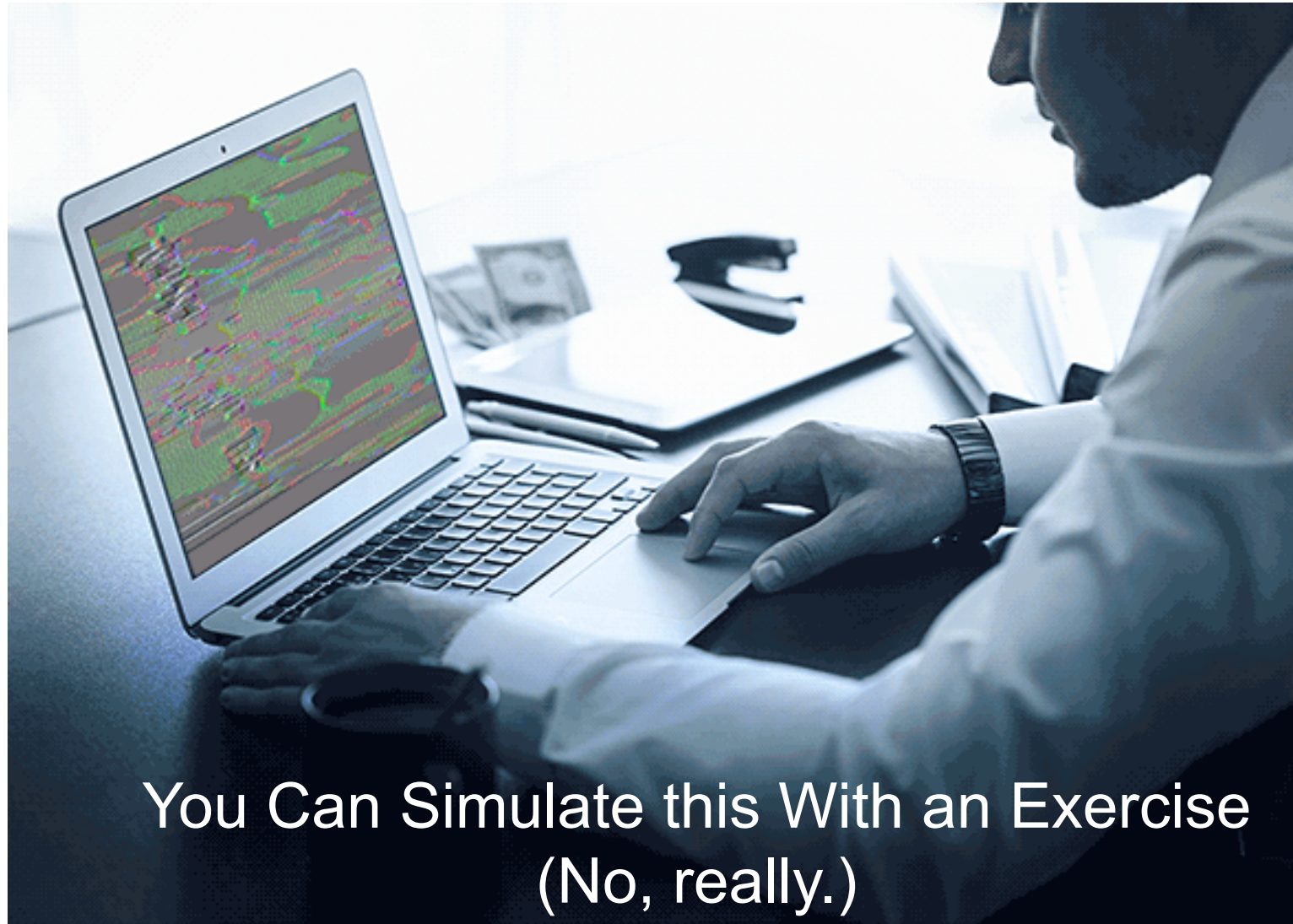
PLEASE HELP

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.)

Start With a Slow Meltdown...

- And then talk:
 - Once the systems become completely unavailable for an unknown amount of time, facilitators in each group can pose questions to each team and begin the discussion.
- The goal is to begin to explore what could be done with limited information.
- Pull out your business continuity plans / COOP and see what type of guidance is provided.

What Will you Find?

- When you ask them what can be done manually, most will say, “Nothing.”
 - You will need to work with them to open their minds.
 - Develop a series of questions to probe the issues.
 - What are your RTOs?
 - Are there workarounds?
 - Brainstorm possibilities.
 - Document your work.
 - After the exercise, expand this work and include in your plans.



It's Only a Matter of Time

Get Going!



- Develop a plan of action to create an *impact*-focused cyber exercise.
 - Really... Right now...
- Tick off each of the eight elements to make your cyber exercise work.
- Get going, REALLY... today!

Thank you

Regina Phelps

Emergency Management & Safety Solutions Inc.

San Francisco, California

415-643-4300

@ReginaPhelps

Regina@ems-solutionsinc.com

www.ems-solutionsinc.com