# Cybersecurity Tactical Simulation (Tabletop Exercise)

## Lessons Learned

SENSATO CYBERSECURITY SOLUTIONS

"Securing our greatest technical assets: Healthcare Information Technology"

NEW JERSEY HOSPITAL ASSOCIATION NJHA

HIMSS New Jersey Chapter

# CTS Event Details

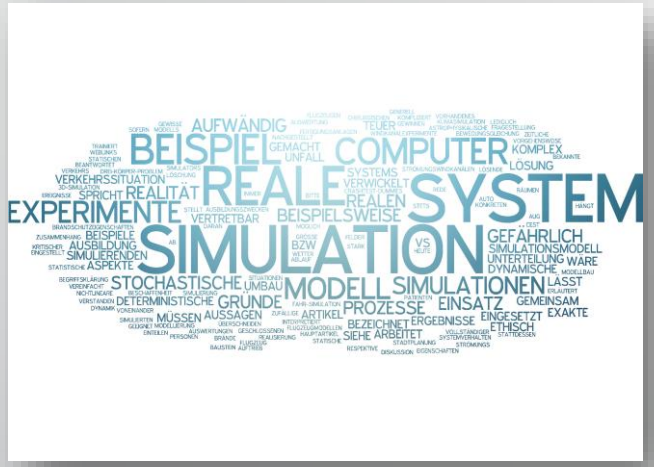
- 13 NJ provider organizations participated over 2 days
- Sponsored by & in partnership with NJHA & NJ HIMSS
- 2 day exercise (March 28 & 29)
- On site at the NJHA Conference Center in Princeton, NJ
- Provided 3 preparation webinars prior to the event
- On day one ½ day was spent on education/level setting
- A cybersecurity update from Josh Liss, Cybersecurity Analyst, NJ Department Homeland Security
- CTS Certificates were issued to all participating providers organizations

# CTS Challenges For Making this Useful for All Participants

- Organizations Participating: 13
- Average Level of Experience: 3 out of 5 *
- Teams with Incident Response (IR) Plans: 5 *
- Teams without IR Teams: 4*
- Formal IR Training: 2*

* Denotes Pre-Survey Responses

# Simulation Approach




**Severity Level:** 2-5 on a scale of 1-5

**Critical Objectives:**

- ✓ Learning and Validation
- ✓ Tipping Point Identification

**Scenario Methods:**

- ✓ Table Top Exercises
- ✓ Full Incident Scenarios

**Four simulation exercises performed over the 2 days**

# Simulation Models

## Tabletop

- Highly Realistic
- Stresses Problem Solving
- Opportunity for Learning and Coaching
- Low Risk to Organizational Operations

## Full Incident

- Highly Realistic
- Involves Extended Teams
- Focuses on Operational Response
- Some Risk to Organizational Operations

# CTS – Lessons Learned From Attendees

- Organizations need to include emergency preparedness staff members since cybersecurity events can impact large scale community safety (i.e. All Traffic Lights Turned Green)
- An Incident may begin in a very harmless low profile way flying under the radar (i.e. minor helpdesk complaints from employees) "Vigilance"
- Be careful not to accuse or terminate staff without doing a proper investigation of facts – They may be the very people you need most!
- In your IR Plan be sure to allow for periodic communication to avoid disruption and maximize focus. (IT staff and other leadership can get overwhelmed with various people wanting a minute to minute update)
- Medical Devices require a few different strategies and air-gapping may be the best at this moment in time. (Air gapping might be a great tool in general!)
- Need one person empowered to make decisions without fear of reprisals Also need a backup person in the event the #1 is not available

# CTS – Lessons Learned From Attendees Continued…

- Don’t assume you are safe from an attack even if your environment is secured. (i.e.US Banking System Compromised)
- Multiple ways of communicating with leadership and staff need to be part of the organization’s IR Plan (i.e. data and communication systems compromised)
- Be sure to have manual operational strategies in your IR Plan as a fall back. Also a good idea to periodically test these strategies.
- As bad as things look or get there is always something that can be done to combat an attack - everyone needs to stays calm and works as a team
- Not every IR Team member will be available during a cyber attack so IR Plans should have both a primary and secondary role assigned


@SensatoCyberSec

Mike Chirico
Mike.Chirico@sensato.co

www.sensato.co
201.637.8287

Joe Carr
Jcarr@njha.com

www.njha.com
609.936.2228