Norwich University Applied Research Institutes
Cyber Security Education/Training and Exercises

October 18, 2013 – University of Memphis
Cyber Security Expo

NARI

National Cybersecurity Preparedness Consortium

Training –

- Cyber Incident Awareness Training
- Emergency Management for IT Professionals
- Cyber Security Exercise Development

Tools –

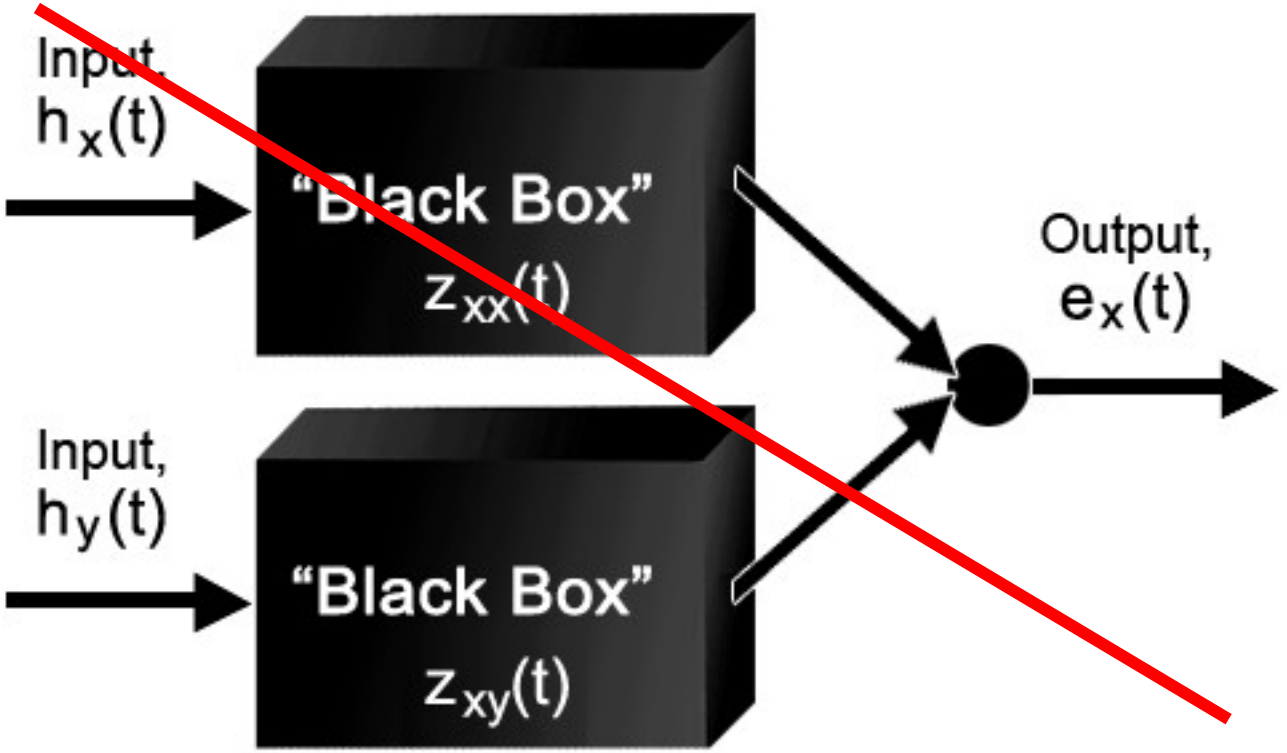
- Cyber Smart – HSEEP Compliant Cyber Exercise Scenario Development Tool

- DECIDE – FS – Distributed Environment for Critical Infrastructure Decision making Exercises – Financial Services

Generation of Success through Experience: Simulation and Exercises

"Tell me, and I will forget. Show me, and I may remember. Involve me, and I will understand." – Confucius, 450 BC

Option A



www-rohan.sdsu.edu

Human in the Loop: Wargaming

Actions have Consequences - Simulation

War Simulators….Key Element of Preparedness

Simulations Prepare Marine Corps for War

1 By U.S. Marine Corps Sgt. Donald Bohanner

2 MARINE CORPS BASE QUANTICO, Va., Dec. 2, 2004 – ….to give Marines the option to use virtual combat training at any time and place courtesy of personal computer-based training.

Benefits of Simulation

- Better decision making
- Team making and team building
- Sharing experiences across a broad groups of teams or individuals.
- Leadership development
- Game-Like & Competitive & Results Driven

Opening to a View of Sector Wide Exercising

- Exercising Allows for Learning and Growth
- Process vs. a Point in Time
- Plan for Improvement and Adjustment
- You Evolve as the Situation and Environment Does
- Failure is an Opportunity

- This is the correct view to take when thinking about preparing your firms for cybersecurity event response

Cyber Exercising

- What is unique about cybersecurity?
  - More akin to Warfare than Security
  - Thinking Game
  - Multiple to Almost Unlimited Attack Vectors
  - Diverse Set of Adversaries with the Offensive Advantage
  - Interactions Matter
  - Plan is Only Good Until the First Impact

History of Quantum Dawn

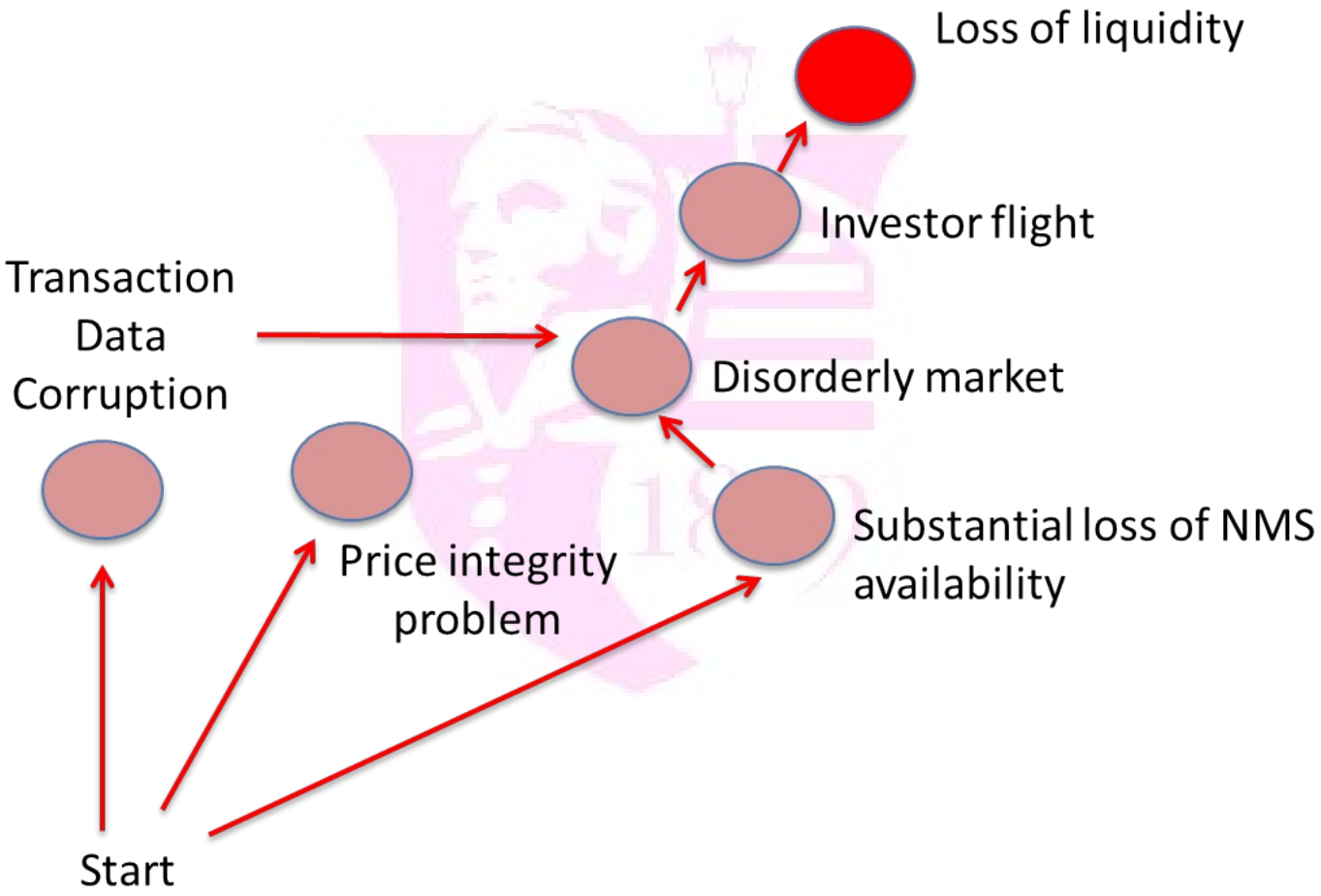
The Basics

- **Date:** July 18, 2013
- **Duration:** One-day, simulating multiple trading days
- **Format:** Distributed functional exercise using the DECIDE-FS® cyber exercise environment simulating a “street wide” cyber attack with a focus on the effects within the equity markets (More to come on DECIDE-FS® later.)
- **Location:** Most firms are participating from their firm locations distributed across the U.S. with exercise control hosted at the SIFMA offices in NY and Regulators in Washington DC.
- **Total Participants:** 50
- **Sector Participants:** 29 Firms, 9 Exchanges, 3 Utilities
- **USG & Other Participants:** Treasury, SEC, Chicago Fed, DHS, FS-ISAC, FSSCC, FSR/BITS, ChicagoFirst, SIFMA
- **Additional Observers:** FBI, OCC, FDIC, FED, FRBNY,
- **After Action Report:** A sector-level AAR will be drafted by Deloitte and player confidentiality will be protected.

Objectives Review

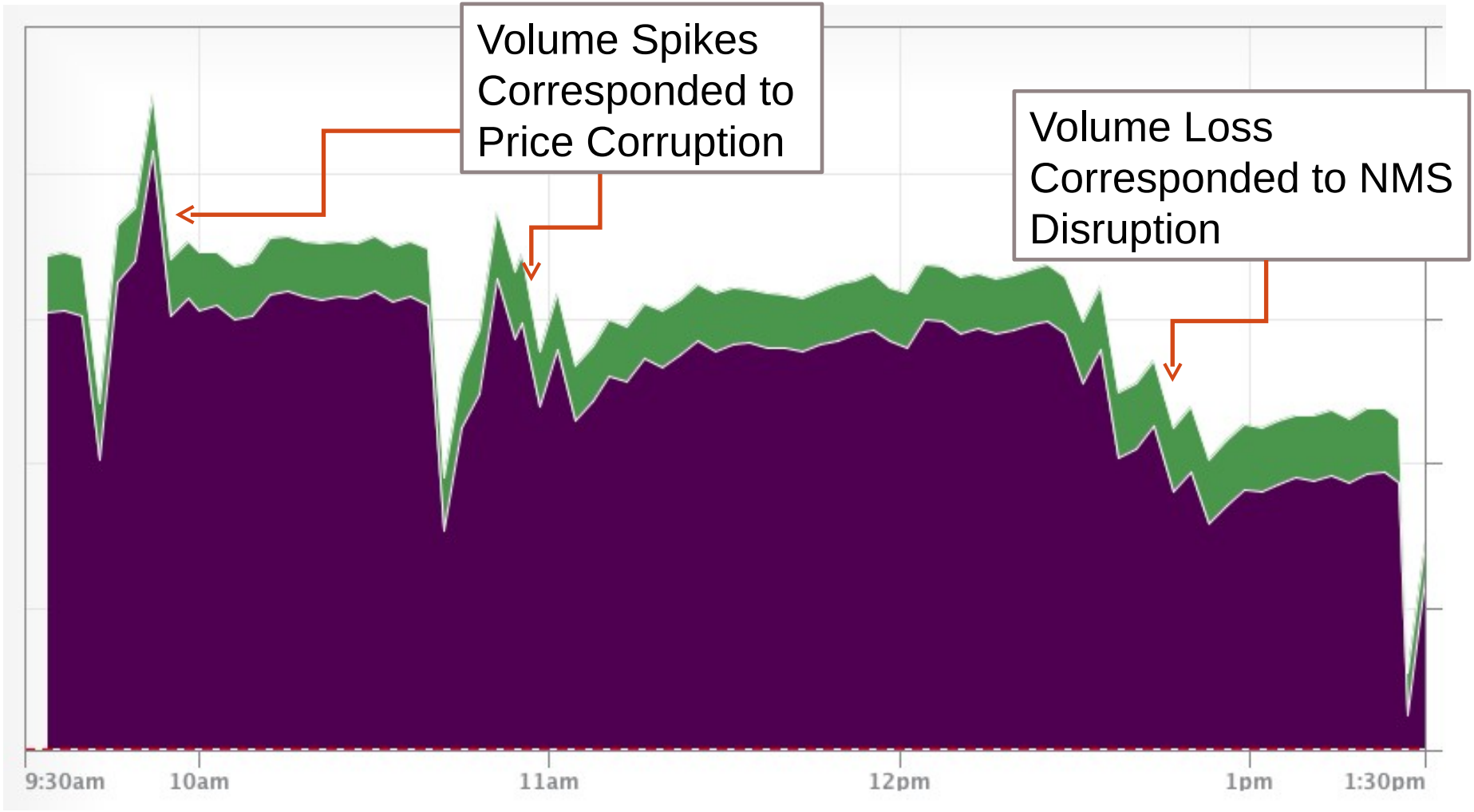
- “You know you’re going to be attacked. You know you’re going to be hacked. You know you’re going to be broken into. Now, what do you do, and how will it impact others?”
- Rehearse internal capabilities in response to a cyber attack scenario and exercise business continuity and information security practices together.
- Exercise sector level entities and improve coordination, communication and crisis-decision-making.
- Simulate the loss of critical infrastructure within the financial services industry
- Develop metrics on the operational readiness of firms, exchanges and infrastructure providers to open and function after an attack.

Example: Quantum Dawn 2 Cyber Scenario



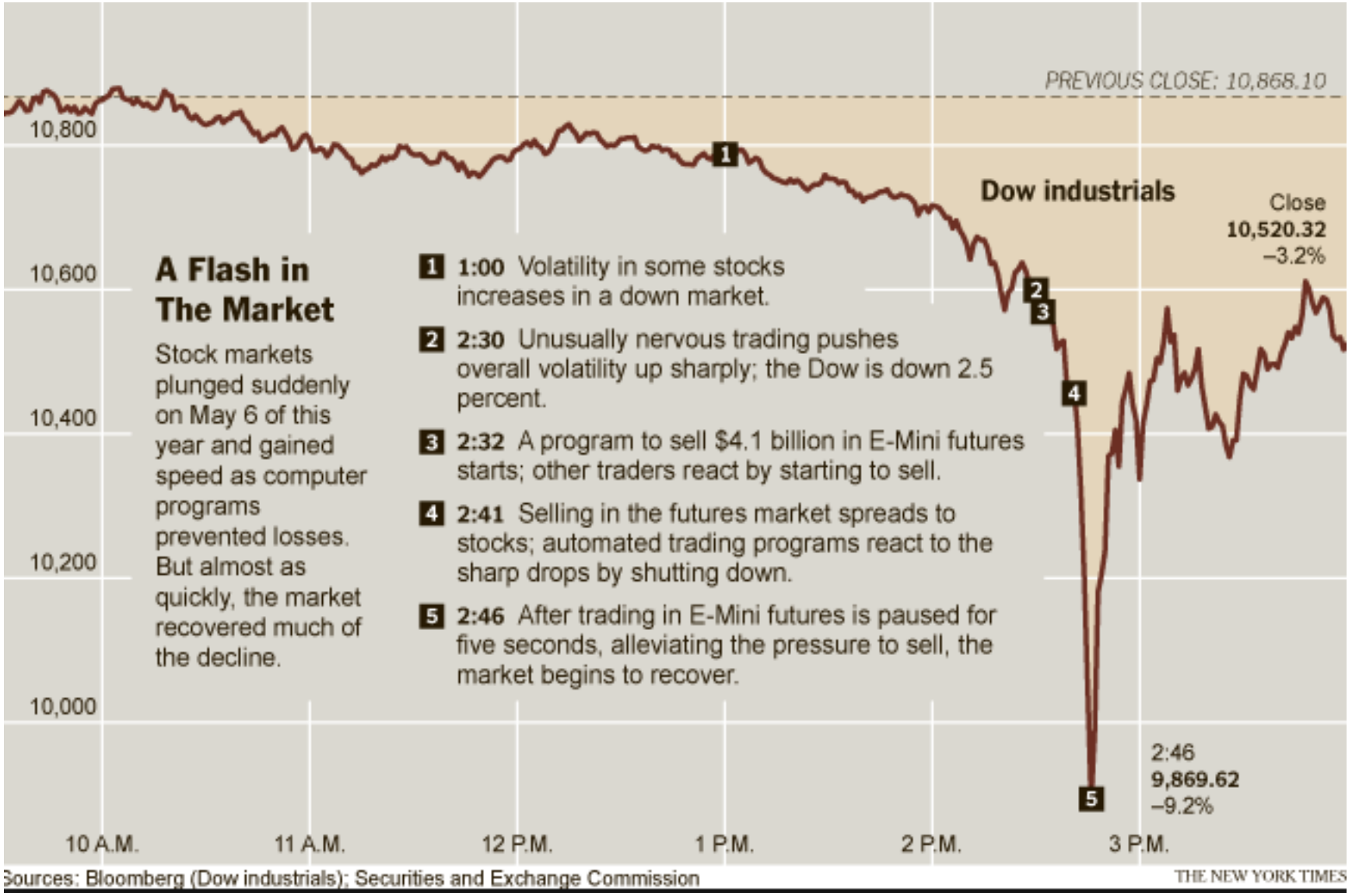
Example: Quantum Dawn 2 Cyber Scenario

Cyber attacks caused this market volume profile



Introduction to A Critical Infrastructure Exercise Environment: DECIDE-FS

May 2010


PREVIOUS CLOSE: 10,868.10
10,800
10,600
10,400
10,200
10,000
Dow industrials
Close
10,520.32
–3.2%
2:46
9,869.62
–9.2%
A Flash in The Market
Stock markets plunged suddenly on May 6 of this year and gained speed as computer programs prevented losses. But almost as quickly, the market recovered much of the decline.
1 1:00 Volatility in some stocks increases in a down market.
2 2:30 Unusually nervous trading pushes overall volatility up sharply; the Dow is down 2.5 percent.
3 2:32 A program to sell $4.1 billion in E-Mini futures starts; other traders react by starting to sell.
4 2:41 Selling in the futures market spreads to stocks; automated trading programs react to the sharp drops by shutting down.
5 2:46 After trading in E-Mini futures is paused for five seconds, alleviating the pressure to sell, the market begins to recover.
10 A.M.
11 A.M.
12 P.M.
1 P.M.
2 P.M.
3 P.M.
Sources: Bloomberg (Dow industrials); Securities and Exchange Commission
THE NEW YORK TIMES

August 2012

Knight Capital 'has 48 hours' to save itself after IT glitch causes $440m loss

Knight Capital is fighting for survival after a $440m (£283.6m) trading loss caused by a software glitch wiped out much of its capital, forcing Knight to seek new funding as its shares plunged as much as 80pc in two days.

August 2013

MARKETS | 8/29/2013 @ 3:25PM | 1,769 views

Nasdaq Details Cause Of Flash Freeze, Says Data Flood Forced Shutdown

http://www.forbes.com

+ Comment Now + Follow Comments

Nasdaq OMX Group NDAQ +0.53% took responsibility for last week's lengthy outage on its namesake stock market, but not without casting some of the culpability toward its chief rival.

(JOHANNES EISELE/AFP/Getty Images)

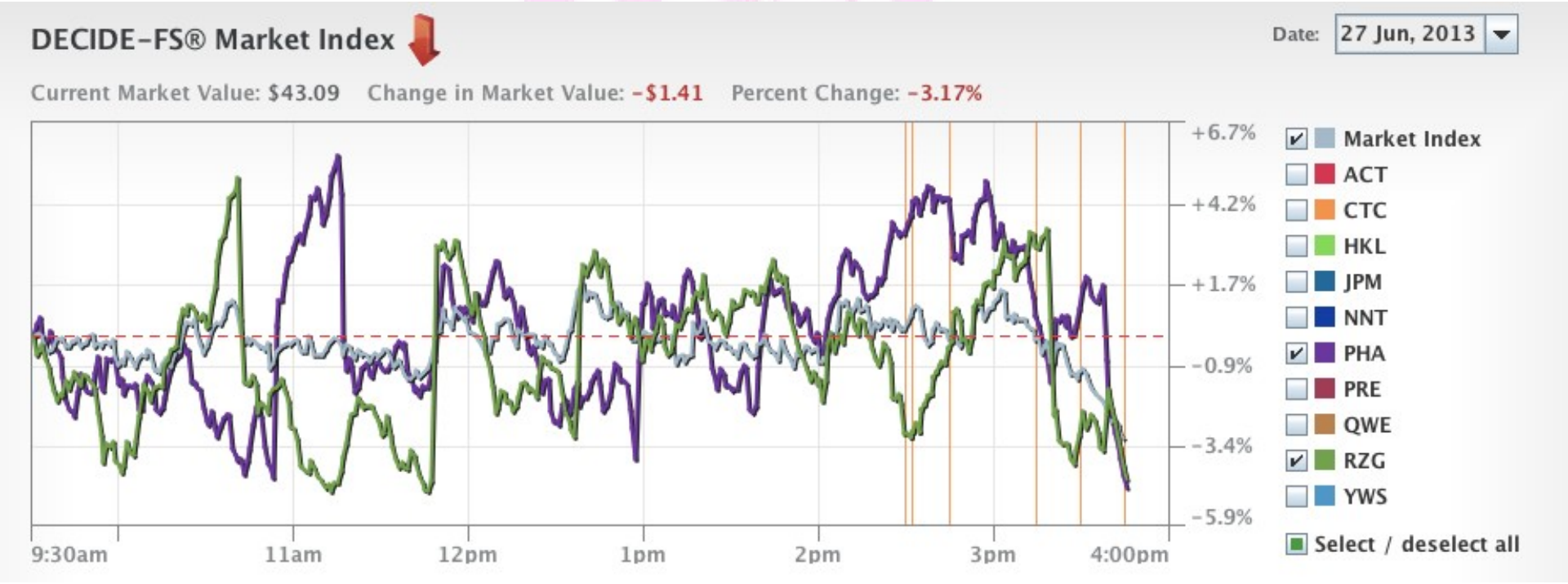
- Not Cyber Attacks –
  - Cost of doing business in a highly connected system
    - Dependent on Technology

DECIDE-FS® Simulation Software – what is it?

- World's first simulation environment designed for financial institutions to create and run cyber disruption exercises
- The intent: facilitate financial industry organizations to think through effective strategies and responses prior to an actual event including impacts caused by actions of counterparties and vendors
- Strong government support and funding using proven technology
- Strong financial industry support extensively tested in live exercises in the finance sector with major stock exchanges and brokerage firms
- Awarded several patents

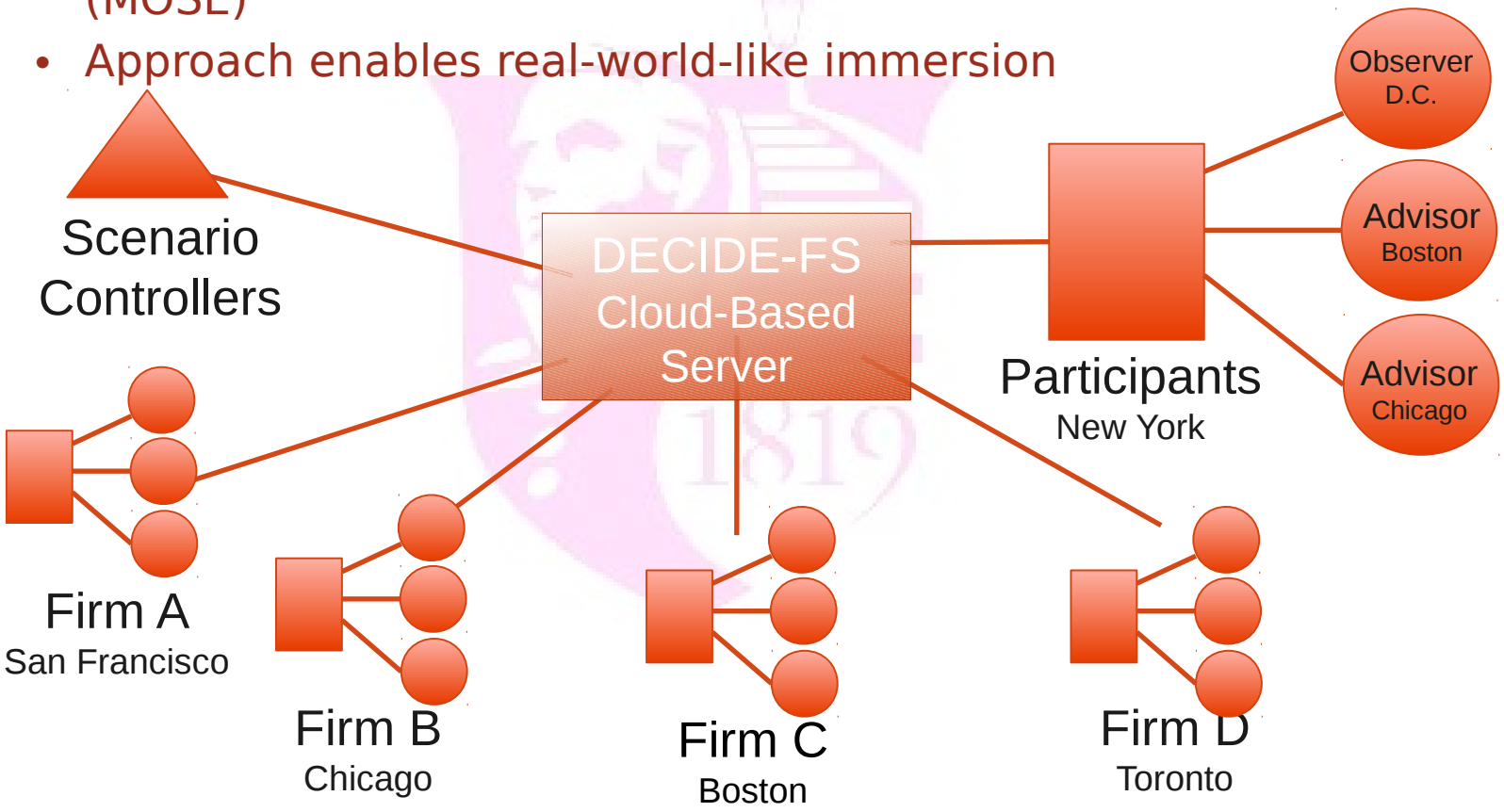
DECIDE-FS® Simulation Software

- DECIDE-FS® simulates the U.S. equities market



DECIDE-FS® Simulation Software

- Interconnected financial organizations in the Quantum Dawn Series represent a Massive Online Sector Exercise (MOSE)
- Approach enables real-world-like immersion



DECIDE-FS® Simulation Software – flexible configuration

- Easy to configure for different sector roles
- Different types of player organizations
  - Broker Dealers, Clearing Firms, Exchanges, Dark Pools, and Clearing Houses
- Players define their simulated business in unique terms
  - i.e. with specific relationships to suppliers and value chain
- Artificial intelligence (AI) agents can play the role of non-participating organizations
- Multi-sector capability
  - Applicable to many critical infrastructure industry sectors
  - Each organization has unique attack vectors and surfaces
  - Participant responses create cascading effects for other organizations
  - Disruption effects appear differently to each simulated organization

DECIDE-FS® Simulation Software – custom scenarios

- Scenario injection that simulates
  - real world news feeds and events
  - operational effects of cyber disruptions
  - natural disasters due to storms resulting in power loss
  - hacker attacks or a nation state attack, APTs or just noise
- Many permutations based on configurations, triggers, and responses
- Organization decisions have consequences
  - Closed feedback loop simulation
- Software provides competitive tension between participants
- Participants can also choose between maximizing profit (front office) and allocating technical resources (back office)