San Francisco Bay Area
Cyber Tabletop Exercise

Situation Manual
June 3, 2014

UNCLASSIFIED

This page is intentionally left blank.

AGENDA

San Francisco Bay Area
Cyber Tabletop Exercise

June 3, 2014 at 9:30 a.m.
San Francisco Police Department Operations Center

9:30 a.m.	**Welcome/Introduction**
9:45 a.m.	**Module I: Information Sharing**
10:45 a.m.	**Break**
11:00 a.m.	**Module II: Response and Mitigation Resources**
12:15 p.m.	**Concluding Remarks**

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

INTRODUCTION

Among the many potential disasters we face today, cyber attacks have become a critical concern. The Bay Area is exposed to unique risks due to the large economic assets located within the region. With a gross domestic product of over $520 billion dollars, the Bay Area is the home to numerous Fortune 500 companies that serve as attractive targets for cyber attackers. Moreover, a cyber incident that results in physical consequences would pose a unique challenge for cyber response and emergency management organizations.

In order to foster information sharing, decision making, and resource management in response to a cyber incident, the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) is currently undertaking the Cyber Playbook Planning Program (CP3) for select Urban Area Security Initiative (UASI) regions. This program serves to enhance Federal, State, local, and private sector cyber response roles, responsibilities, and coordination mechanisms—with an emphasis on integrating private sector and critical infrastructure partners into community or jurisdictional cyber planning.

The Bay Area CP3 program focuses on the creation of a regional Playbook to be used in the event of a severe cyber incident. The Playbook should explain how key partners will coordinate information sharing, decision making, and resource management in response to a cyber incident. As the starting point for Playbook development, NCCIC, in coordination with the Northern California Regional Intelligence Center and regional Bay Area partners, designed and developed a scenario-based cyber exercise to identify key agencies and resources, and to assess current state of preparation. This tabletop exercise will address coordination, information sharing, and collaboration between public and private sector stakeholders.

Objectives

1. Examine the capabilities and authorities of regional public and private sector partners in responding to a significant cyber incident with physical consequences.
2. Examine the effectiveness of information sharing and collaboration across public and private sector entities in the Bay Area.
3. Inform the development of a regional Playbook to aid in coordinating a response to real-world cyber incidents.

Format

The Bay Area Cyber Tabletop Exercise is a 180-minute facilitated discussion involving public and private sector partners throughout the San Francisco Bay Area. The exercise will be supported by a facilitator. ***Discussions will be unclassified but not for attribution***.

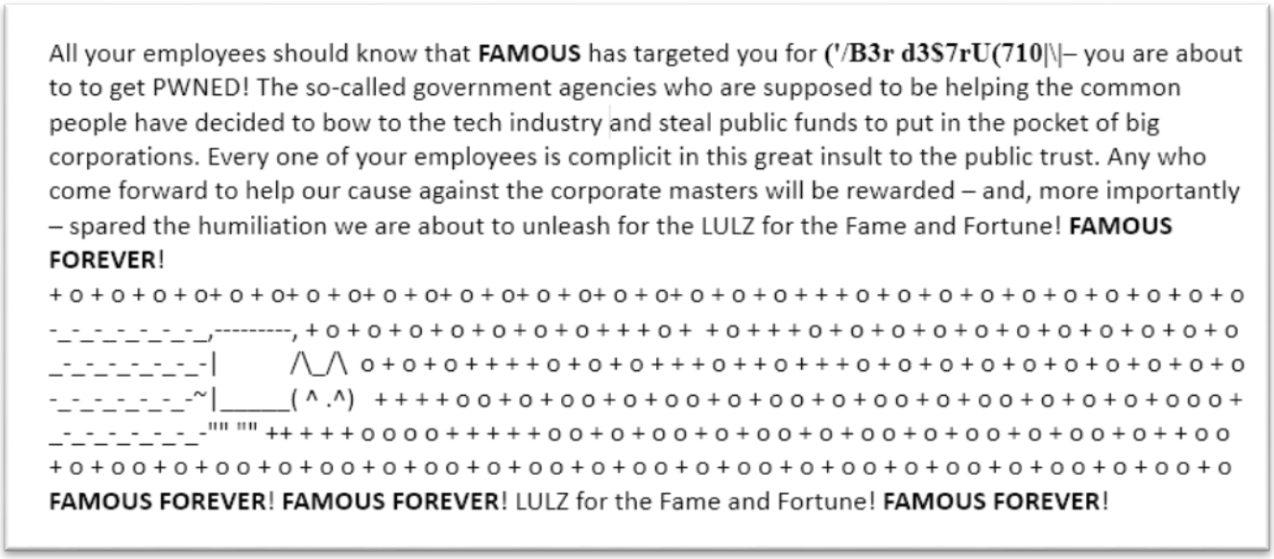
Assumptions and Artificialities

The Bay Area Cyber Tabletop Exercise condenses a complex situation in the interest of achieving exercise objectives within the scheduled timeframe. The extreme, simultaneous nature of the threats described is intended to generate discussion. It does not reflect any current threat assessment.

The Ground Truth Scenario is designed to apply to all the participants. For example, rather than single out one or two Bay Area organizations, the scenario is designed to have every participant consider the threat as it would affect their organization. Thus, when the scenario documentation describes "your organization," participants are invited to consider the scenario as it relates to *their* organization.

GROUND TRUTH SCENARIO: MODULE I

Beginning at 7:00 a.m. Pacific Daylight Time (PDT) on June 2, 2014, a hacktivist group known as FAMOUS sends emails to every employee in your global address book, insisting that your organization is complicit in a "conspiracy to cheat the poor and middle class of services in order to line the pockets of the Silicon Valley tech giants." The email warns that FAMOUS will destroy your organization, and encourages your employees to join FAMOUS against the "corporate masters."


All your employees should know that **FAMOUS** has targeted you for **('/B3r d3S7rU(710|\|**– you are about to to get PWNED! The so-called government agencies who are supposed to be helping the common people have decided to bow to the tech industry and steal public funds to put in the pocket of big corporations. Every one of your employees is complicit in this great insult to the public trust. Any who come forward to help our cause against the corporate masters will be rewarded – and, more importantly – spared the humiliation we are about to unleash for the LULZ for the Fame and Fortune! **FAMOUS FOREVER**!

FAMOUS FOREVER! **FAMOUS FOREVER**! LULZ for the Fame and Fortune! **FAMOUS FOREVER**!

On June 3, 2014, your internet-facing systems intermittently experience a peak 350Gbps Distribution Denial-of-Service (DDoS) attack, disabling websites and slowing internal web access and traffic. Within a few hours, systems throughout your organization begin to fail, their hard drives wiped and their BIOS flash memory corrupted. The Information Technology department in your organization suspects a destructive virus as the source, but impacted systems leave no trace to examine. Automated Heating, Ventilation, and Air Conditioning (HVAC) systems in your building also begin experiencing unusual temperature fluctuations.

In addition, the following entities have access to specific information:

- **United States Secret Service** – a highly-placed criminal informant inside FAMOUS has provided detailed technical specifications for a new DDoS tool. The information is known only to a handful of leaders in the FAMOUS group.
- **Federal Bureau of Investigation (FBI)** – The National Cyber Investigative Joint Task Force has classified information indicating *Nation State X* has developed a Shamoon-like cyber weapon that exploits a very common software vulnerability. The FBI is working with the

cooperative software vendor who requests that no notice of this vulnerability be revealed outside of the Department of Justice until a fix is available.

- **Northern California Regional Intelligence Center** – Multiple agencies in the region have noted unusual network activity indicating abnormally high botnet activity.
- **FEMA Region IX** and **California Office of Emergency Services** – Unusually warm weather coupled with wildfire damage to power lines in certain areas has left area electrical grids vulnerable to brownout and blackout conditions.

MODULE I: ISSUES FOR DISCUSSION

The following questions are designed to assist participants in preparing for questions that will likely emerge during Module I of the exercise discussion.

1. In the event that you find evidence of an attack on your networks, consider the following:
   - What decision-making process would you follow before notifying any external party?
   - With whom would you share the information you gathered?
     - Through what channels?
     - To what end?
2. If an attack is ongoing somewhere else in the Bay Area (or national) ecosystem, how would you expect to learn of it?
3. For the government partners, if you have obtained intelligence about an impending or ongoing attack:
   - How and with whom would you share it?
   - Could you assist affected partners in responding to the incident?
   - If so, how?

GROUND TRUTH SCENARIO: MODULE II

By the close of business on June 3, websites across the Bay Area are experiencing failures from the DDoS attack. Email systems for these organizations are also sluggish or inoperable for extended periods of time.

In addition, a large and growing number of systems across the Bay Area have failed completely from the suspected Shamoon-like virus.[1]

By 7:00 p.m. PDT on June 3, the following consequences are occurring across the Bay Area:

- Water pipelines experience a failure of control systems. Bay Division Pipelines Nos. 1 and 2 experience a loss of positive pressure, causing a "boil water advisory" condition in the following areas:
    - San Francisco
    - San Mateo
    - Redwood City
    - Palo Alto
    - Mountain View
    - San Jose
- Traffic light control systems in the City of San Francisco have failed, causing severe gridlock for homebound commuters.
- Automated HVAC systems in major buildings in San Francisco and Oakland begin turning themselves on and off suddenly, causing brownout and blackout conditions in some areas. Blackouts affect the transmission and delivery of electrical power. As a result, telecommunications networks experience outages, and public transportation is severely impacted.
- Combinations of gas delivery system failures and electrical outages leave thousands of residents needing pilot light relights.

Table 1: Cities Affected by Gas System Failures and Electrical Outages

City	U.S. Census Data Population Estimates
Berkeley	115,403
Oakland	400,790
San Leandro	86,890

[1] The Shamoon Malware, also known as a Disttrack or W32.Disstrack, is an information-stealing malware that also includes a destructive module. Shamoon renders infected systems useless by overwriting the Master Boot Record, the partition tables, and most of the files with random data. US CERT—Shamoon/DistTrack Malware Report

MODULE II: ISSUES FOR DISCUSSION

The following questions are designed to assist participants in preparing for questions that will likely emerge during Phase II of the exercise discussion.

1. If the attack you are experiencing exceeds the capabilities of your internal response resources, consider the following:

   - To whom do you turn for assistance?
   - Through what channels?
   - Are there partners within the Bay Area that you would be coordinating and collaborating with on finding a solution to these issues? Formally or informally?
   - Are there partners within the State that you would be coordinating and collaborating with on finding a solution to these issues?
     Are there partners within the Federal Government that you would be coordinating and collaborating with to find a solution to these issues?

2. Emergency management organizations:

   - If your area of responsibility is experiencing physical consequences, would that fact change your available resources or your authority to act?
   - If so, how?
   - Do you have the capability and/or authority to respond to the cyber cause of the physical incident?

3. All participants:

   - In the event of a region-wide, ongoing incident, how will Bay Area partners create unity of effort in their response and mitigation initiatives?
     a. Will there be an incident command structure established regionally?
     b. Who is "in charge," and of what?
        i. Coordination
        ii. Decision making (e.g., companies vs. regulators)
        iii. Investigation
        iv. Critical infrastructure protection and assistance
     c. How will coordination occur?
        i. Physical collocation?
        ii. Virtual coordination through a portal such as the Homeland Security Information Network or WebEOC?
        iii. Other?
   - How is information communicated to the public? When? Through what channels?
   - How is mutual assistance established locally?
     a. Does mutual assistance include cyber incidents?
     b. What is the process to request assistance from the State of California for cyber response and mitigation?

PARTICIPANTS

- Alameda County Sheriff's Office
- Archdiocese of San Francisco
- Bank of America
- Bay Area Rapid Transit
- Bay Area UASI
- Berkeley Police Department
- California Army National Guard
- California College of the Arts
- California Department of Justice
- California Governor's Office of Emergency Services
- California Highway Patrol
- California Information Security Office
- California Military Department
- California State Threat Assessment Center
- California Water Service Co.
- California Water Service Group
- City College of San Francisco (CCSF)
- City & County of San Francisco
- City of Mill Valley
- City of Monterey
- City of Newark Police Department
- City of Oakland
- City of Roseville
- Contra Costa County Fire Protection District
- Contra Costa County Health
- Cooley LLP
- County of San Mateo
- Dell SecureWorks
- Emergency Management and Safety Solutions, Inc.
- Federal Bureau of Investigation
- FEMA Region IX
- Filipino American Law Enforcement Officers Association
- FireEye
- Fresno County Sheriff’s Office
- Hillsborough Police Department
- InfraGard & USF
- Intuit Inc.
- JPA
- L-3 Communications

- Leidos BDR
- Livingston Police Department
- Metropolitan Transportation Commission
- Mirage Systems
- Monterey County
- Mountain View Police Department
- NCI Security LLC
- NetSuite
- Northern California Computer Crimes Task Force
- Northern California Regional Intelligence Center
- Pacific Gas and Electric
- Pacifica Police Department
- Port of Oakland
- Oakland International Airport
- San Francisco Dept. of Emergency Management
- San Francisco District Attorney
- San Francisco Municipal Transportation Agency
- San Francisco Police Department
- San Francisco Police Credit Union
- San Jose Police Department
- Santa Clara Valley Water District
- Silicon Valley Regional Computer Forensic Lab
- Square, Inc.
- Surface Transportation Security Inspection Program (STSIP)
- Symantec
- U.S. Department of Homeland Security
- U.S. Secret Service
- United States Coast Guard/PACAREA