



Homeland
Security



BAY AREA CENTER FOR
REGIONAL DISASTER RESILIENCE



Bay Area Cyber Resilience Workshop

Held May 15, 2015 at the Alameda County Office of Emergency Services, Dublin CA

Overview and Outcomes

Representatives from utilities, government agencies, businesses, non-profits, and community institutions convened on May 15 at the Alameda County Office of Emergency Services in Dublin to learn how they could build capabilities and capacity across key performance areas related to IT security, operations, and business continuity to improve organizational and regional cyber resilience. The workshop was sponsored by the U.S. Department of Homeland Security's (DHS) Office of Cyber Security and Communications in the National Protection and Programs Directorate, in partnership with the Northern California Regional Intelligence Center (NCRIC), and the Bay Area Center for Regional Disaster Resilience (BACRDR), which also hosted the event.

Workshop Purpose

The impetus behind the workshop was heightened concerns about increasing and expanding cyber attacks on the operational and business systems that run the Bay Area's critical infrastructures and other essential services. The workshop goal was to provide managers in all critical infrastructure sectors with a better understanding of cyber threats and security and resilience concepts, and actions to protect against and mitigate attacks and disruptions impacting operational and business systems. The workshop also was intended to overview cyber security and resilience activities underway by the Northern California Regional Intelligence Center (NCRIC) with local agencies, the Bay Area UASI, and the U.S. Department of Homeland Security. An important workshop objective was to gain feedback from regional stakeholder organizations on useful activities that could assist them in making their organizations more cyber resilient. Another key objective was to recruit interested organizations in current and future regional activities, including a recently established Cyber Work Group facilitated by the Bay Area UASI.

Format and Agenda

The workshop format and agenda were designed to give participants:

- An appreciation of the current cyber threat from a regional perspective (presented by NCRIC Deputy Director Dan Mahoney), and
- Guidance from U.S. DHS cyber experts led by Deron McElroy, Director of Regional Partnerships and Cybersecurity Advisor at DHS. DHS experts provided practical and demonstrative examples of cyber resilience capability building over and above improvement

of IT security controls and countermeasures, as well as information on current trends in protecting and sustaining IT services related to core operational and business functions and missions. The experts also addressed decision criteria for cyber incidents, vulnerabilities, and business continuity and provided other useful information related to risk-based decision-making and security planning to improve the resilience of critical IT services.

The last portion of the workshop provided a status report on current Bay Area activities focusing on cyber resilience by NCRIC Lead Cyber Analyst Elizabeth McCracken and David Frazer, Bay Area UASI Risk and Information Sharing Project Manager. The workshop culminated with a discussion among participants and presenters facilitated by Frazer and BACRDR Executive Director Paula Scalingi to identify ideas and recommendations for priority actions that can build on ongoing activities to further Bay Area cyber resilience. *(See Appendix A for the workshop agenda. Workshop presentational materials and other cyber resilience resources can be accessed through the following DropBox link for additional details:*

<https://www.dropbox.com/sh/lw5mv3y4ddlajeh/AADSx0bPTvMh1K8M96G1DLoBa?dl=0>

Workshop Outcomes

Ideas and Recommendations for Follow-on Activities raised by Participants

These included:

- **Expansion of the Bay Area UASI-facilitated Cyber Focus Work Group** to include interested private, public sector, and non-profit organizations.
- **A Cyber Resilience Workshop Series.** Potential topics suggested for training events included—
 - Drilling down on current cyber threats and consequences and what cyber resilience requires;
 - Individual sector cyber security and resilience concerns and needs (e.g., healthcare, financial services, and electric power);
 - Security of lifeline infrastructure control systems;
 - Inclusion of cyber resilience in all-hazards preparedness risk assessments and disaster response and recovery planning;
 - Continuity of local government IT services, including emergency and public safety services;
 - Education for IT personnel on the needs of emergency managers, public health, and other first responder constituencies;
 - Methods and options for cyber resilience in the event of a disruption that impacts Emergency Operations Center (EOC) operations during an emergency or incident;
 - Cyber resilience awareness for local elected officials, such as city managers;
 - Engaging cyber security expertise and setting up cyber mutual aid agreements.

- **Inclusion in Golden Guardian and Urban Shield exercises of cyber-disruption components;**
- **Incorporation into annual San Francisco Fleet Week activities of cyber resilience awareness training;**
- **Guides on cyber resilience**
 - For emergency managers on cyber response and recovery;
 - For community and business leaders on the importance of cyber resilience and what it requires;
- **A credentialing program for IT experts** to assist with response and initial recovery post-incident;
- **Creation of a Bay Area Cyber Resilience Alliance** to facilitate regional information sharing/coordination and to build relationships/promote and enhance cyber security and resilience.

Next Steps

Participants were told they would be provided with an overview of the workshop, which would summarize participant ideas and recommendations for follow-on activities. Participants interested in joining the regional Cyber Security Work Group were encouraged to contact David Frazer, the Bay Area UASI facilitator for the Work Group.

For further information, please contact David Frazer, Bay Area UASI, 707-565-1108 or david.frazer@Sonoma-County.org, or Paula Scalingi, Executive Director, Bay Area Center for Regional Disaster Resilience, 925-399-6229 or pscalingi@BayAreaCRDR.org

Appendix A: Workshop Agenda

Welcome and Introductions

Paula Scalingi, Executive Director, Bay Area Center for Regional Disaster Resilience

Opening Remarks

Dan Mahoney, Deputy Director, Northern California Regional Intelligence Center (NCRIC)

Enhancing Organizational Cyber Resilience

U.S. Department of Homeland Security (DHS) Office of Cybersecurity and Communications

Session 1: Overview of Workshop, Cyber Threats, and Cyber Resilience and its Benefits

Session 2: Identifying IT Services and Managing the Assets that Support Them

Session 3: Protection and Sustainment of Assets

Session 4: Managing Business Disruptions: Service Continuity & Incident Management

Session 5: Managing for Cybersecurity Success

Session 6: Recap of Key Topics and how to get Additional Help and Information

Status of Regional Cyber Resilience Activities

David Frazer, Risk and Information Sharing Project Manager, Bay Area UASI

Elizabeth McCracken, Lead Cyber Analyst, NCRIC

Potential Follow-on Activities to Build a Cyber Resilient Bay Area

Facilitated discussion among participants with NCRIC and DHS presenters

Appendix B: Participating Organizations

AC Transit	NC 4
Alameda County Public Works Agency	Northern California Regional Intelligence Center
Alameda Hospital	NetApp
Archdiocese of San Francisco	Paul Coleman Consulting
BART	PG&E
Bay Area Center for Regional Disaster Resilience	RSA/EMC
Bay Area UASI	San Francisco
Chinese Hospital, San Francisco	<ul style="list-style-type: none">• Department of Emergency Management• Department of Public Health
CITRIS	San Joaquin County Public Health Services
City of Alameda	San Mateo County
City of Dublin Police	SF CARD
City of Mill Valley	SSL
City of Oakland	Stanford Graduate School of Business
City of Union City	Tetra Tech
Comcast	U.S. Department of Homeland Security
Contra Costa Health Services Hazardous Materials Programs	<ul style="list-style-type: none">• Office of Cybersecurity and Communications• Software Engineering Institute
CR Solutions	U.S. Department of Veterans Affairs
D.W. Morgan	<ul style="list-style-type: none">• Office of Information and Technology• San Francisco Medical Center• Veterans Health Administration
East Bay Regional Parks Police	U.S. Geological Survey
EBMUD	UCSF Benioff Children's Hospital Oakland
FBI	University of San Francisco
FEMA Region IX	VMware
First Federal Savings and Loan Association of San Rafael	Wells Fargo
Kaiser Permanente	
Lawrence Livermore National Laboratory	