Update on NCRIC Cyber Security Unit for the Bay Area UASI - May 8, 2014

Background

The NCRIC Cyber Security Program is expanding from a single analyst providing strategic analytic products, to a team of five that will additionally conduct training, outreach, vulnerability/risk assessments, and incident notification and response.

The UASI provided approximately $400,000 towards staffing three of these positions. At present, two individuals have begun employment in their assigned roles, while the third has been selected and is pending completion of the standard law enforcement background investigation.

Notable Accomplishments by NCRIC Cyber Security Unit in past 9 months:

Training

- Developed, organized, and hosted a 16-hour Law Enforcement Cyber Investigation course for 25 law enforcement officers, as well as a 4-hour Private Sector Cyber Incident Response course for 30 incident response professionals.
- Developed the 40-hour Cyber Intelligence Analyst Course at the National Computer Forensics Institute (NCFI) with DHS and the U.S. Secret Service. Over 100 students have been trained over five sessions of 20 students each.
- Organized the Bay Area Cyber Exercise, to occur on 2014-06-03, for both private sector and public sector partners (e.g. SLTT law enforcement agencies). The purpose of the Cyber Exercise is to examine cyber incident response and information sharing capabilities within the Northern California region. It is anticipated the event will yield valuable information that will assist the NCRIC and the Department of Homeland Security develop a "Cyber Playbook" designed to assist the participants and other organizations in responding to a major cyber incident. This exercise will also inform future regional and Statewide Cyber Exercises to come.

Incident Response

- Responded to the Cryptolocker malware and attack campaign, which affected numerous organizations in the region. Assisted with mitigation and response, and produced a Cryptolocker mitigation product for partners to help them better defend themselves.
- Facilitated mitigation when a local hospital was overwhelmed by telephony denial of service attack
- Conduct phishing attack evaluation and analysis, separating false positives from true positives

- Responded when a local law enforcement agency's website was defaced: obtained and analyzed information on perpetrator, then referred to FBI when international source was confirmed
- Currently engage with the State CISO's office on incident notification and mitigation throughout the state, usually within 12-hours.
- Responded to a resurgence in Quakbot infections: coordinated statewide notification among fellow fusion centers, notified victims and provided actionable mitigation strategies. Several entities were not aware of their compromise and expressed gratitude for the assistance

Outreach

- Facilitate relationships with California CISO, National Guard, DHS, and more
- Briefed all CSU CISOs on cyber threats, trends, and government partnerships
- Bi-monthly strategic briefing on current trends, tactics, events in cyber security
- Regularly brief major organizations, both public and private, on the cyber threat.
- Produced in-depth threat assessments on specific threats or vulnerabilities to the NCRIC AOR (Insider Threat, Swatting)

Projects and Deliverables planned for next 9 months:

Risk Analysis

- Vulnerability Assessments, determine internal network devices that may become compromised and act as vectors or pivots for further harm; provide actionable reports and consultation for reducing risk
- Penetration Testing: assess perimeter defenses and internet-facing systems against known exploits or malware

Network monitoring

- Near real-time analysis of partner external firewall traffic, providing automated alerting and applicable defensive actions