California Public Utilities Commission

Key Takeaways from 2016 Safety En Banc

I. Top Six Takeaways:

1. All interconnected critical infrastructures have one thing in common: human beings, interacting with each other within their organizations, with other organizations, and with technology.
2. “Human error” should not be viewed as a way of ending inquiry by assigning blame for an event, but as an opportunity to engineer the environment in which people work to reduce the impact of human factors.
3. The internet is a crucial element of interconnected infrastructure. However, state agencies, particularly PUCs, lack subject matter expertise in cybersecurity.
4. It is unclear what the Commission’s responsibilities and resources would be during a crisis, and whether we would be self-directed or directed by another agency.
5. Unknown unknowns are an ongoing challenge, e.g., knowing which stakeholders to invite to formal exercises and informal exchanges of information.
6. There need to be more opportunities for stakeholders to come together and learn from each other in informal settings, perhaps on neutral ground such as an academic institution, before a crisis.

II. Takeaways from Each Session:

a. Session 1

1. Communications between interested stakeholders includes communication with the Commission, but it is unclear what the proper forum is for addressing interconnected infrastructure issues, as well as how much information needs to be shared. For example, the Commission is not an emergency operations center; we need to know that AT&T is working with BART, but to what degree?
2. Communications services will never be restored as quickly as you want during a crisis. A proper incident command structure allows personnel to respond immediately without waiting for communications to be restored.
3. Situational awareness between all parties and across all silos needs to be built before a disaster strikes. During the fog of war, it is too late.
4. Some participants report limited visibility with respect to risks outside of their own respective operations, and would welcome opportunities for additional information-sharing.
5. There was no consensus as to whether events that begin as a cyberattack or other hostile act rather than as a branch hitting a transmission line require different coordination and response.

b. Session 2

1. Interconnected infrastructure providers have vastly different lifecycles. Traditional utility companies may be investing for decades, while software companies may have product lifecycles and investment windows measurable in months. This growing disconnect in institutional

planning and investment philosophy between interconnected stakeholders creates more opportunities for human error, and makes close coordination more essential.

2. Different industries and different regions of California adopt new technology at different speeds. Some companies are using new technology on equipment that is 40 or 50 years old; others may be unknowingly relying on technology that is no longer supported by the manufacturer.
3. Technology has the potential to increase reliability, but also creates new risks. There are benefits to replacing handwritten gas pressure charts with digital records, but hostile state actors couldn't hack those handwritten charts.
4. Low tech, old school technologies may still have a role to play in the event of a catastrophe, especially if older technologies are retained strategically as part of resilience/back-up rather than simply as a default.

c. Session 3

1. There are groups that exist for information sharing and threat assessment, e.g. federal Fusion Centers, but the Commission is not a part of those groups. Should we be? How many of these groups exist, and how much overlap is there?
2. The Commission has rules requiring emergency prep for utilities; do we have similar rules for ourselves? Do we take direction from another agency, e.g., CalOES?
3. The Commission has an opportunity for a systematic evaluation of our processes, rules, jurisdiction, what we can and cannot do during an emergency; with the new Division of Safety Advocates and the SED Risk Assessment group, we may have the staff.
4. The regulatory role is up front, in preparation and planning, not in disaster response.
5. Hindrances to emergency response may be found in unexpected places. When old equipment or structures used by first responders are destroyed during an incident, CEQA rules may thwart its rapid replacement; California income tax rules may hinder the use of out of state personnel for mutual aid.
6. Unregulated companies have declined to participate in government cybersecurity exercises because they feared that doing so would constitute consent to being regulated. How can government be a "conveyor" without regulating?
7. Whether or not there are "safe spaces" to discuss shared concerns, reporting cyberattacks does not feel "safe" to some stakeholders.
8. In an emergency, there is a tension between maintaining confidentiality and minimizing risk/impact. In the Incident Command System there can be a liaison whose role includes receiving information from people who want to remain anonymous.