Purpose

The major goal of this document is to provide a starting point for electricity subsector executives, managers, information technology, risk management, critical infrastructure operations, and regulators to discuss the appropriate role for cloud computing in their environment and how it should be managed.

Background

In the past isolation has been a keystone in the protection of critical infrastructure components (e.g. command and controls), providing some degree of control over the impact a careless user, unpatched machine, or poor network management could have on operations. Such isolation, real or perceived, is becoming less and less a viable, believable choice for several reasons—the interconnectedness of the Smart Grid and Cloud Computing being at the top of the list.

The inroads made by Cloud based hosting and communications continue to expand; driven by public and investor pressures to reduce operating costs and by the relentless marketing of cloud products and services that promise a secure and reliable computing capability with lower manning, minimal oversight, and substantial cost savings. The growth of using cloud or cloud-like capabilities, coupled with the ever growing necessity of interfacing critical infrastructure components (e.g. command and control) to a wide assortment of data sources, means that there will be direct and indirect two-way connections between the infrastructure and cloud components. *(actual hosting of critical infra on cloud)*

"Cloud" is used to refer to hosting and communications services provided by a source not directly under the control of or dedicated to the operation of a specific critical infrastructure segment. These services might include public cloud based infrastructures, applications developed and hosted by a third party, operational data provided by a third party, or hosting accomplished by an internal general purpose datacenter. In this context we can expect to need to evaluate the use of these resources to directly provide critical infrastructure services or how to ensure the safety of an interface between these services and our critical infrastructure.

The public is certainly aware of cyber threats to the cloud. Security specialists realize the threats are more pervasive, wide-ranging, and dangerous than the media has reported. Information stored on the cloud is vulnerable as traditional methods of storing information reside in a single location and travels over one path. New technologies exist that protect information on the cloud as a complete data set that is never in one place and never travels over a single network path as data is distributed across multiple locations with military grade encryption and access to the data requires authentication/authorization by the network administrator. The challenge is making security specialists aware of new technologies across all critical infrastructure industries.

The problem is network and software engineers at critical infrastructure institutions are in a continual battle to keep up with the tremendously varied and constantly escalating stream of attacks aimed at the cloud. Software and hardware vendors providing security products and protection for these organizations work around the clock, identifying, isolating, and trying to mitigate the damage of signaling attacks, and other hacking and electronic theft schemes launched by an ever-increasing number of sophisticated cyber terrorists and thieves. Clearly this strategy is no longer sustainable.

This paper considers and recommends alternatives that can vastly simplify the tasks of securing and managing the cloud by utilizing next generation tools and processes incorporated in the SOC (security operational centers) for command and control.

Considerations and Recommendations

- Sample use cases that are relevant to the electricity subsector will be included in this section, such as:
    - Samples cover where we might see proposals to *host core mobile cloud computing (MCC) services* in "cloud" and *"feeds" into our C&C* that are likely from "cloud" (include future)
        - Data center facility
        - Monitoring (Include electricity subsector examples) (is there an electricity subsector example)
        - Network facilities
        - Data storage and backup
        - Client care (Include electricity subsector examples) (is there an electricity subsector example)
        - Physical security
        - Provisioning
        - Security policy
        - Privacy policy
        - DRP/SIRT/Change Management
        - Etc…
        - Distributed management – multi-tier SOC architecture for C&C
    - State of guidance today (strong infrastructure, but not necessarily explicit "cloud" app)
        - State of art facility processes
        - State of art maintenance processes
        - State of art security processes.
        - Etc..
        - State of art Processes are converted into data for historical forensic analysis for managing, securing and reporting the effectiveness of the processes. This is known as information management today. This methodology is utilized in all software systems today for predictive command and control.
    - Next Level of Thinking or next level information management.
        - Processes are a set of tasks defined in a graphical cause and effect relationship.
        - The ability to audit each task according to the pre-defined cause an effect graph would enable real time command and control for effective mediation.
        - The ability to use data dispersion and dispersed virtual datacenters
        - Aggregation of computational storage and transmission resources of cloud computing into globally dispersed hybrid multi-technology networks

    - Context specific "thinking points" from among many- mapped to use case example where we might see it. e.g.
        - **Internal data centers** that have a growth/general purpose focus and lack experience or knowledge of how to isolate or manage critical components
            - **Lack of visibility provided by software tool- raw event logs**
            - **Lack of Process know how or the inability to connect the dots..,**
        - Lack of insight or accountability without appropriate contract
            - **Externally developed and hosted mission critical apps** that aren't necessarily run in the flashy new data center we saw in the tour—a portion run by lowest bidder. (Example: emergency scene management app sent earlier)

- **Inadequate isolation of mission critical functions** from non-MCC systems when IAS or PAS
    - “Droplet in the Cloud” email sent earlier- unpatched server among many compromises gateway for breach of seemingly unrelated systems
    - Recent Java weaknesses easily exploited and possible compromise of management systems regardless of OS
    - DOSS thru systems, storage, or network components shared with general components
- Application of general purpose computing “best practices” , not controls commensurate with the criticality of the function being hosted/provided
- Dangers of having traditional non-dispersed data located in one location and unprotected data regardless if traditional non-dispersed encryption is in place

- SAS/PAS/IAS: DON’T JUST ACCEPT AN SLA, SPECIFY WHAT YOU NEED AND VERIFY— Define your requirements and write a contract with specs and strong oversight/compliance requirements, verify capability, do PCA and audit, …
  (The SLA alluded to by one of the participants in the telecom two weeks ago would be nice—really interested to see if it provides adequate detail and oversight, also curious about how it says to enforce…)
- INTERFACES: WHAT DO YOU DO TODAY? Given the Texas model and the growth of organization owned energy management and storage, there has got to be some work on this already.

Close

- RISK CANNOT BE TRANSFERRED—no matter who hosted or provides the service, failures come back to those charged with providing the service to the public. (FERC information on investigations and reporting can be added here if needed for backup)

References