Current Risk Management Practices

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Organizations that develop national/international standards for critical infrastructure need to ensure that the standards/practices that protect critical infrastructure are mandatory to implement. There should be adequate penalties/consequences to ensure adoption of the standards/practices.

Specific Industry Practices

1. Are these practices widely used throughout critical infrastructure and industry?

The use of encryption does exist in critical infrastructure networks, however the practice is not ubiquitous and should be made mandatory. While many network providers claim that private or virtually private networks are secure, the logical segmentation techniques that form the basis of these security claims offer no direct protection of data. Encryption is the only way to protect data –both information and control, as it travels over network infrastructures.

Encryption is often eschewed due to perception that it will cause performance and availability issues, neither are tolerable within critical infrastructures. However, Encryption technologies have evolved and today's next generation encryption uses group based policy definitions and key distribution which eliminate most or all of the management and performance issues often associated with this form of security.

There are two facets to creating a transparent but robust security overlay for critical infrastructure. The first is the use of purpose built encryptions appliances, which not only ensure high-speed, low-latency processing but also help to define the electronic security perimeter (ESP), the demarcation between trusted and un-trusted networks.

The second is centralized policy and key management (as opposed to link by link configuration). Not only is centralized management more efficient but it also ensures that cyber policies are followed and allows for much easier and more accurate reporting.

In combination, these two facets of group encryption also allow for the decoupling of network security from the networking infrastructure. This separation of duties is of vital importance on critical infrastructure because it allows for the best practice of separating network administration from security enforcement, making it especially difficult for a single actor to compromise the network from within.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

Encryption is the most critical for operation of a critical infrastructure network. As stated in point 1, encryption is the only way to ensure data is not compromised in transit. When combined with on going authentication, it is the only way to ensure the secure and accurate delivery of verified control commands, and protects systems behind the enforcement points by discarding frames or packets that have failed authentication.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

Encryption is applicable in all sectors that have sensitive data or control commands traversing over any shared or externally accessible networks.

5. Which of these practices pose the most significant implementation challenge?

Encryption has traditionally been an implementation challenge, especially in large mesh networks – depending on the solution implemented. Latency was often the biggest issue. Next generation encryption solutions with purpose built appliances, however, simplify the implementation of scalable encryption and are non-disruptive to performance and monitoring.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

Experience has shown that unless a standard or guideline is mandatory, adoption of security is negligible as resources are diverted to other mandatory requirements or to discretionary projects. Given the known vulnerabilities, the ease with which they can be exploited, and the consequences of a breach, mandatory adoption of network encryption (even over so called private networks) is warranted.