Why must India implement security systems for the power sector?

Recently, the Indian Power Business Association has come to an agreement that it will deploy a comprehensive firewall system, combined with many other security measures.

In the context of the internet and popular cross-platform connectivity technologies developed today, any field can become the target of cybercriminals as well as malicious agents in cyberspace. , causing immeasurable damage.

Recently, the Indian Power Business Association has come to a consensus that it will deploy a transparent firewall system, combined with many other security measures, to prevent early attacks on public systems. their information technology and check all security incidents related to electricity system management and operation systems nationwide.

As such, power grid operators and regulators will need to have a synchronized, continuous, practical plan in case their network gets hacked, according to a draft rule. published by Central Indian Power Regulatory Commission. This is in fact a revolutionary innovation, complementary to the regulations in the management and management of the national grid system that was coined decades ago.

The decision to establish a digital defense system for the Indian national power grid came just months after a nation's nuclear power producer admitted its system was breached by an attack. public networks cause relatively serious consequences. The case, like a 'spill of water', shows the need for further action to protect the management systems of businesses operating in the electricity sector - one of the vital areas for real in any country, and at the same time closely related to national security.

Actual statistics have shown that energy corporations around the world are becoming the favorite target for hackers due to their large profits and serious consequences that could happen if a hack is targeted. These companies are successfully implemented. This is the reason that motivates governments and especially businesses to take serious safeguard measures.

Central, state power transmission management facilities as well as load dispatch centers are required to implement sensitive data protection systems and clearly report the availability of reserve power transmission. in the event of a cyber security incident that causes partial system paralysis. Along with that is monitoring and reporting on the level of security risks periodically.

It is also recommended that these agencies prioritize qualified resources and allocate a sufficient workforce for online security needs.

To deal with malware, India will deploy its central grid protection system based on multiple interwoven firewalls, combining operational management isolation from office networks to limiting risks with human factors.

India's approach should be replicated around the world in the context of the increasingly complex cyber security situation.