Written by Lila Kee, chief product officer, GMO GlobalSign Inc

CYBERSECURITY

EXAMINING THE US APPROACH TO CNI CYBERSECURITY FOR THE POWER GRID

Cybersecurity threats to any nation's power grid poses real risks to both the reliability and safety of businesses and citizens whose everyday lives rely on energy to run their economy and vital services

Since post-9/11, both the EU and US have taken on cybersecurity initiatives that involve a common approach for Critical Infrastructure (CI) sectors, such as in the case of energy by developing guidelines on how owners, operators and regulators should implement preventative measures aimed at mitigating maliciously driven cyber-attacks. The European Programme for Critical Infrastructure Protection (EPCIP) has taken the lead in developing a central approach to cybersecurity of CI sectors for European stakeholders, whereas the US energy sector follows voluntary and mandatory guidelines from a range of government and industry agencies.

THE US APPROACH TO CYBERSECURITY

This approach is risk-based and, like all risk, a certain level must be accepted as a balance among costs, operation impact, usability and security must be realised. The key of course is sizing the right level of security to the level of exposure associated with the risk. Cybersecurity initiatives taking place in the US attempt to perform that balancing act and although yet to be proven, seem to be on the right track.

After a series of false legislative starts, in February 2013, the Obama Administration issued an Executive Order (EO) called Improving Critical Infrastructure Cybersecurity, with the hope of engaging CI owners and operators in developing, promoting and implementing cybersecurity best practices.

The Executive Order states "…a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security".

Two key points stressed in the EO are:
1. Increased Information Sharing: federal agencies are now required to share unclassified reports of threats to US companies by expanding the voluntary Enhanced Cybersecurity Service programme that is tasked with providing near real-time sharing of cybersecurity threats. This expanded audience now includes companies that fall under the government's classification of Critical Infrastructure. 2. Development of Cybersecurity Framework: the National Institute of Standards and Technology (NIST) has been appointed with the task of creating a Cybersecurity Practice Framework in collaboration with CI stakeholders that will be used to reduce threats.

Securing the US power grid is of upmost importance to the White House and, naturally, electricity generation, transmission and distribution are identified as key CNI areas that are expected to benefit from adopting the cybersecurity framework.

SOLICITING FEEDBACK

Similarly to the EU, the majority of power grid assets are owned and operated by the private sector, therefore NIST is prudent to heavily engage the electric industry, the government and industry standards boards and regulators, and the vendors that serve them to support the development of the cybersecurity framework.

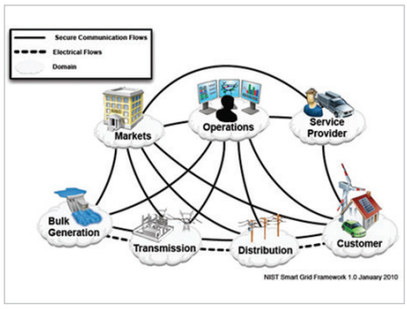
The fourth of a series of engagement meetings held by NIST this month completes the goal of soliciting feedback from these key stakeholders to help shape the final framework expected to be announced in early 2014. Once finalised, CI participants will be encouraged to voluntarily adopt the best practices and standards.

INCENTIVES TO ADOPT THE FRAMEWORK

In fact, the White House recently announced a series of incentives that it is considering to

"By 2035, 80 per cent of America's electricity will come from clean energy sources."
President Barack Obama, State of Union Address, 25 January 2011.

CYBERSECURITY



promote the quick adoption of the framework.

Some of the incentives being considered include: cybersecurity insurance – build underwriting practices that promote the adoption of cyber risk-reducing measures and risk-based pricing and foster a competitive cyber insurance market. Grants – incentivising the adoption of the framework and participation in the voluntary programme as a condition, or as one of the weighted criteria for federal critical infrastructure grants. Process preference – agencies offered suggestions on a range of government programmes in which participating in the voluntary programme could be a consideration in expediting existing government service delivery. Liability limitation – possible reduced tort liability, limited indemnity, higher burdens of proof, or the creation of a federal legal privilege that pre-empts State disclosure requirements. As the framework is developed, agencies will continue to gather information about the specific areas identified in the reports related to liability limitation.

NIST'S APPROACH TO THE FRAMEWORK

A key to NIST's approach to this framework is to include existing proven standards into the framework. One such standard already identified is the North American Energy Standards Board (NAESB) Standard on Public Key Infrastructure (PKI) for the Wholesale Electric Quadrant, WEQ-012.

Today, NAESB's standards development for Public Key Infrastructure (PKI) applies to participants involved in market-based applications that serve power generation and transmission within the Wholesale Electric Quadrant. The Federal Regulatory Energy Commission (FERC), which regulates the US interstate transmission of natural gas, oil and electricity, is in the processes of receiving comments on WEQ-012 and if adopted as a final rule, will become mandatory for entities under FERC's jurisdiction.

NAESB's approach to standards development nicely aligns with the goals of the Obama's Cybersecurity Executive Order by: encouraging industry, vendor and government collaboration; optimising the balance of security, operational implementation and cost appropriate for risk of breach; fluid to deal with a rapidly changing threat landscape; enhances accountability by being enforceable (when federally mandated by FERC).

The EU should take note of the approach NIST is taking to developing the Cybersecurity Framework when developing its own methodologies around securing Power Grid IT and SCADA resources and communications. As the (Smart) grid modernises, increased innovation, productivity and efficiency gains are inevitable however, often at the risk of leveraging IP and the internet.

Referring to January 2010, NISTs Smart Grid Framework showed that a secure communication flow between stakeholders was crucial in securing its infrastructure.

Going forward, our governments should continue to promote the continued streamlining of energy distribution and use, however they should also provide the industry with the right tools to counter the new and ever-advancing cyber vulnerabilities these innovations bring.

Strong authentication of users (systems and people) is just one area of cybersecurity, but an essential one that if not implemented securely can have potentially devastating impact.

"By 2035, 80 per cent of America's electricity will come from clean energy sources," said President Barack Obama at the State of Union Address on 25 January 2011.

What happened? In May of 2013, Chinese hackers compromised a US Army database that contained information on 84,000 dams that were considered a significant hazard if they failed.

PREVENTABLE BREACH

Access was given to an unauthorised individual without the proper level of access for the information. If cybersecurity measures that required strong two-factor authentication were in place at the time then this breach might have been prevented.

Unfortunately, the reality of resistance to change, adoption of government guidelines and the perception of costly measures that do not really enhance security, is prevalent on either side of the pond. EU governments, academia and industry should keep a watchful eye on how the US security framework unfolds. Steps in place suggests a good balance between industry-government information sharing, regulations and steep consequences where the stakes are high, and a voluntary-based system that focuses more on carrots and less on sticks is a sure-fire measure to get real security improvements vs check-box compliance.

FURTHER INFORMATION

www.globalsign.co.uk/enterprise

GlobalSign Enterprise Security Solutions

GlobalSign has been a trust service provider since 1996 and focuses on providing convenient and highly productive PKI solutions for organisations of all sizes. Its core Digital Certificate solutions allow customers to conduct SSL-secured transactions, data transfer, distribution of tamper-proof code and protection of identities to secure email and access control.

With the increasing expectations of protecting critical system functions and infrastructure, GlobalSign understands the importance of implementing security solutions that will help protect networks, control access and protect critical data. With the continuous advancements in technology and ever-changing security regulations, it can be seem to be time-consuming and costly.

GlobalSign's range of security solutions encompassing the use of Digital Certificate technology are not only reliable, scalable and cost-effective, but can meet the CI stringent standards and security controls for online transactions and authentication to support specific markets and system function.