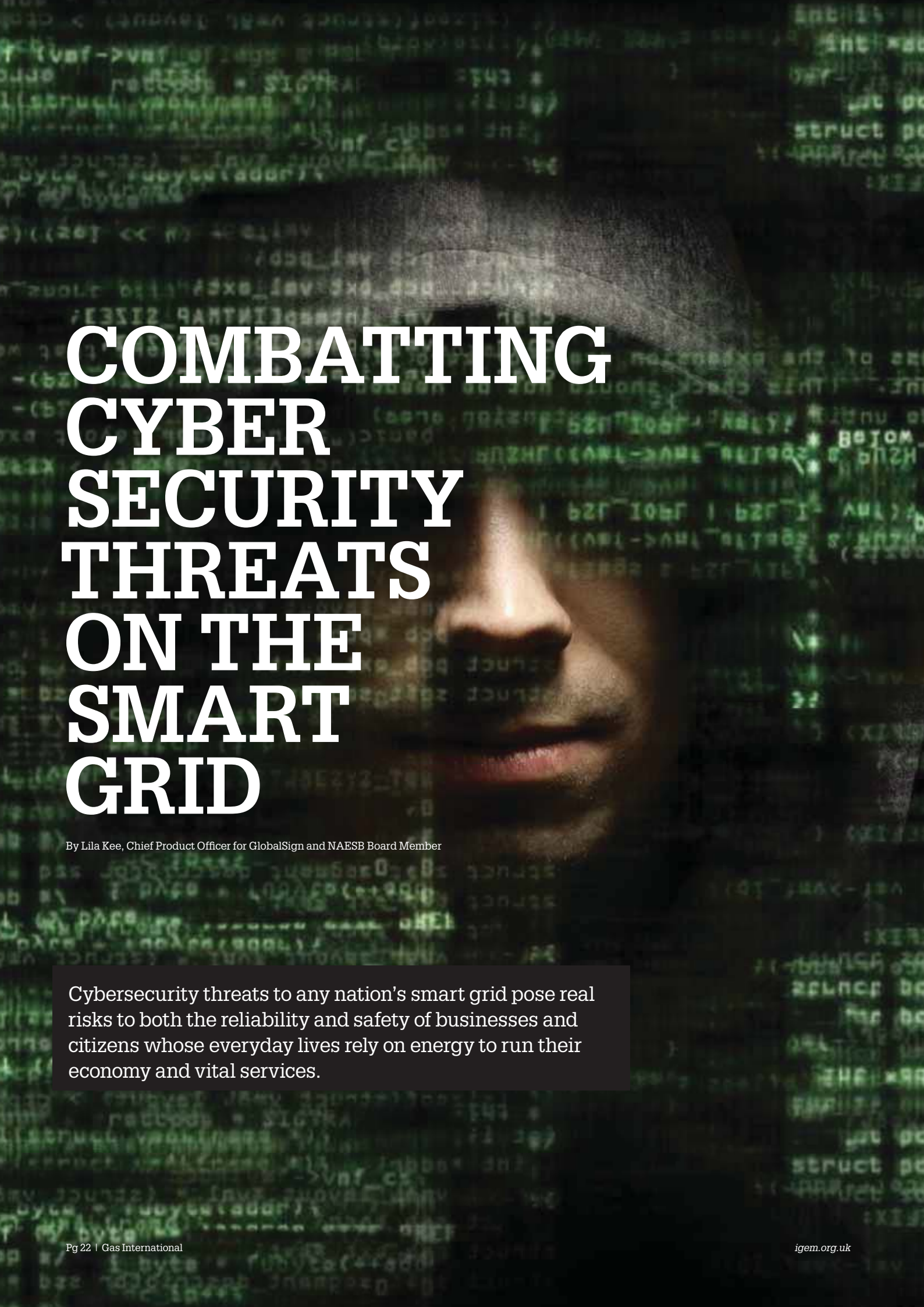

COMBATTING CYBER SECURITY THREATS ON THE SMART GRID

By Lila Kee, Chief Product Officer for GlobalSign and NAESB Board Member

Cybersecurity threats to any nation's smart grid pose 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.

Recognising that even a temporary shortage of energy supply could result in significant economic loss, or worse yet possible loss of life, the US government has identified energy as one of its critical national infrastructure (CNI) sectors.

Post-911, both the EU and the 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 cyberattacks.

Recent headlines and mounting evidence suggest that cyberattacks on critical systems are increasing. Cybercriminals have identified electric utility grids as prime targets for disruption activities and of all the identified CNI sectors, the energy industry is the recipient of a disproportionate number of cyber-related attacks.

Hackers prey on systems in desperate need of modernisation which, if penetrated, could lead to devastating consequences. As a result, CI cybersecurity has become a prime concern for both governments and citizens alike.

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.

Hackers prey on systems in desperate need of modernisation which, if penetrated, could lead to devastating consequences

The impact of the internet of things

Many CIs are managed, controlled and accessible in today's world via internet-connected systems, making them vulnerable to cyberattacks. One can hardly speak of the internet of things without including the smart grid in the discussion.

Considering the sheer volume of interconnected and highly distributed machine-to-machine communication, the benefits of automated energy management seem endless. However, like most internet based transmissions, the benefits of efficiency, cost savings and convenience invite malicious actors to either corrupt smart grid systems for financial gain, or worse; cause devastating outages and/or destruction, especially in transactions void of human involvement. Continued standards development around cybersecurity, in particular device authentication, is paramount in securing the smart grid.

Improving security with the use of public key infrastructure

In the wake of increasing attacks, US CIs in particular are stepping up efforts to amplify their cybersecurity and strengthen their defenses. In recent months, US wholesale energy participants have shown that CI providers can strengthen cybersecurity by implementing a standard-based public key infrastructure (PKI).

A PKI enables users of an unsecure public network (i.e., the internet) to securely and privately exchange data through the use of encryptions obtained and shared through a trusted authority.

The US energy sector contains more than 6,413 power plants (including 3,273 traditional electric utilities and 1,728 non-utility power producers) with approximately 1,075 gigawatts of installed generation. Electric power providers, the wholesale energy market, regulators and market participants are embracing PKI as a secure, scalable, flexible and cost effective method to securely authenticate the many digital identities involved in the wholesale electricity market.

Independent Systems Operators (ISOs), which coordinate, control and monitor electrical power system operations from state to state, are using PKI standards developed by the Northern American Electricity Standards Board (NAESB) to strengthen security for their cyber-based business processes and transactions.

However, due to the many implementation details involved, if the PKI technology is not executed correctly it can also produce a vulnerable system. NAESB members have worked together to produce a standard for the wholesale energy sector based on best practices, proven management techniques and advanced digital certificate technologies.

Recommendations

Certificate authority GlobalSign is urging smart grid equipment and software manufacturers, as well as operators, to step up efforts to upgrade technology, especially around the area of replacing weak passwords with stronger authentication measures.

As in any cyber security planning, IT and security professionals should incorporate the level of security necessary for the associated risk of a breach. In the case of smart grids this risk is potentially catastrophic. As participants in the NAESB, GlobalSign is also encouraging energy participants to incorporate cybersecurity standards developed by the board and the North American Electric Reliability Corporation (NERC), that if adopted will lead to a safer smart grid ecosystem.

Conclusion

While most CIs have recognised that they need improved cyber defences, they have not yet made the tremendous strides forward that the energy sector has made. Many ISOs in the energy sector recognise the value of cybersecurity frameworks, and are adopting PKI practices using the demonstrated standards developed by NAESB's cybersecurity sub-committee developed using shared expertise from both the public and private sectors.

In the US President Barack Obama's recent executive order, the National Institute of Standards and Technology (NIST) was directed to lead the effort to develop a cybersecurity framework that would consist of adopting industry best-practices wherever possible. As part of NIST's draft cybersecurity framework, the NAESB standard on PKI stands a good chance of being applied to other CI sectors.

With regards to protecting the CNI in the EU, the European Programme for Critical Infrastructure Protection (EPCIP), which is leading the EU initiatives for European stakeholders, could potentially benefit from this recent US development. ■

For more information about NAESB visit *www.naesb.org*
For further information about how GlobalSign provides authentication solutions for the energy sector visit *www.globalsign.co.uk/verticals/energy.html*