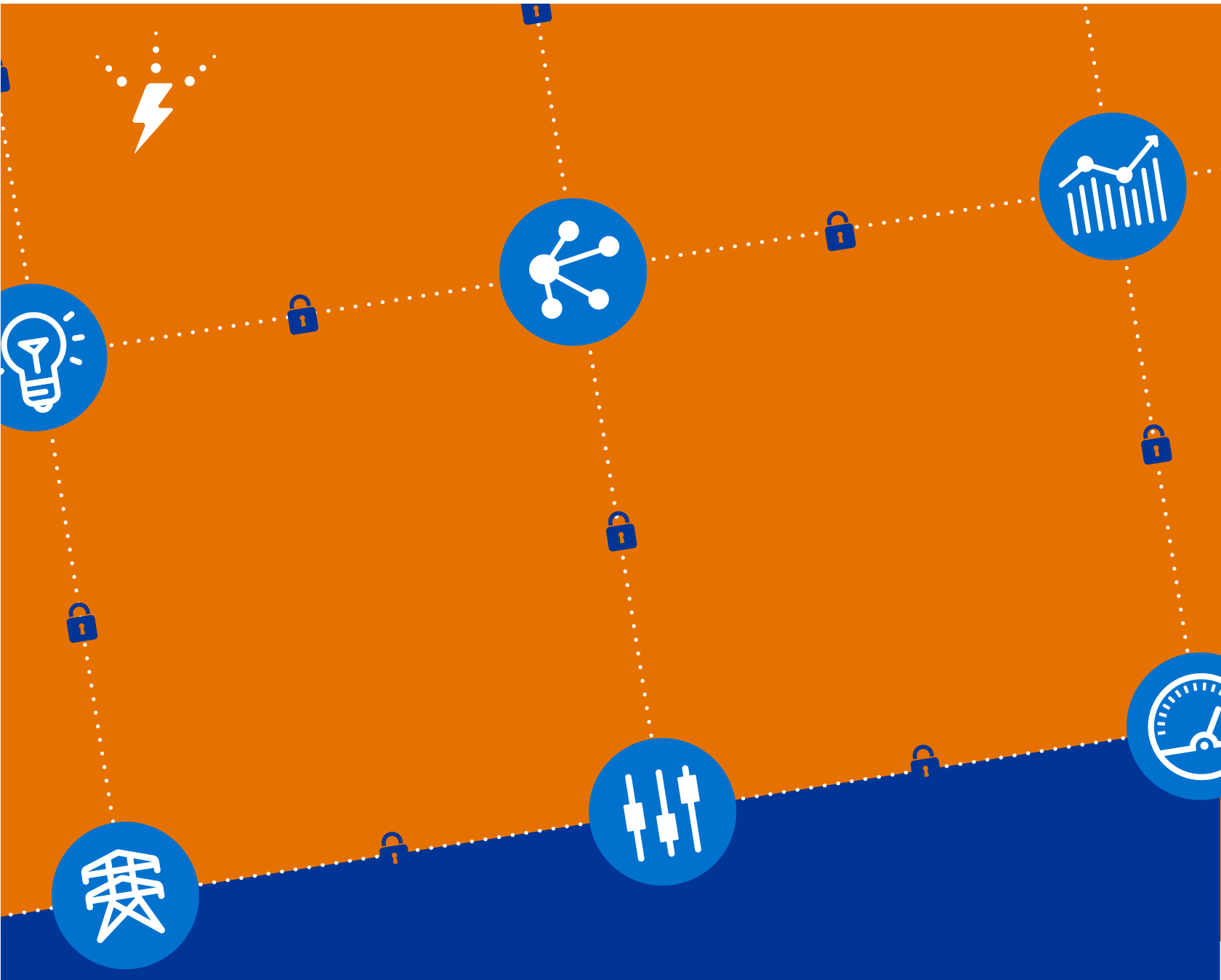
Nothing's out of reach.



GRID MODERNIZATION:

Cybersecurity

SENSUS
a xylem brand

Cybersecurity must stay at the forefront of activity because technology is constantly changing the grid and electricity distribution.

Cybersecurity is a growing threat to the grid. "In the last few years, there have been an increasing number of attacks on grid systems in Europe and other global markets, including state-sponsored attacks on US utilities," explains Balu Ambady, director of security technologies at Sensus. "These attacks, in addition to the past decade or so of cyberattacks on retailers and banks, are constantly in the news and continue to raise the concerns of consumers." Moreover, it's one thing to consider a read-only meter being hacked, but with expanding smart-home technologies and their associated in-home devices, security concerns take on new dimensions, especially with two-way communication that allows large number of devices to be controlled remotely.

In addition to customer-driven fears, which are a top concern for electric utility companies, grid operation security is a top-line matter. There are also new regulatory requirements that are compelling utilities to comply with more stringent privacy regulations, such as GDPR in EU. However, it's a grave error for utilities to believe that compliance alone ensures security.

As utilities and communities around the country take on the latest industry push for grid modernization efforts, there is a focus on the grid edge and network resiliency. However, cybersecurity must stay at the forefront of activity because technology is constantly changing the grid and electricity distribution.

Concerns, threats and deficiencies

According to Ambady, today's utilities share similar security concerns in the areas of confidentiality, integrity and availability.

Confidentiality pertains to data privacy and is the factor most top of mind for utility consumers. This generally includes personal data privacy and protecting meter-read information from eavesdropping.

Integrity has to do with ensuring that data is not tampered with on the customer end or on the utility end. In other words, this facet prevents the meters or communication systems from being rigged to alter the reading and, therefore, the consumer's bill. "With the older AMR systems, there were limits on what a hacker could do," says Ambady. "But with devices getting smarter and remote connectivity increasing, there's a greater potential of hacker reset or shutoff. So, utilities must ensure that command and control capabilities are authorized and cannot be corrupted."

Every utility has the same three primary security concerns.

Confidentiality

Integrity

Availability

Availability, on the other hand, is the singular security aspect that has been present since the inception of electric lights: consumers expect their power to be on. But today, availability goes beyond consistent delivery per consumer service expectations to also include consistent data accessibility. Utilities need to be able to consistently and accurately read meters to bill those customers receiving power.

Like most industries, utilities only recently have had to consider cybersecurity issues as a top priority. But the exponential increase of threats over the past decade is progressively disconcerting for consumers, corporations and governments alike. There are several deficiencies for utilities when it comes to embracing the level of cybersecurity required today.

The first issue involves legacy systems—networks and endpoints. Devices coming to market over the past five years or so typically have advanced capabilities such as end-to-end encryption, so these are less of a concern. And equipment that is over 20 years old doesn't really pose a threat either, because everything is mechanical and wired with little cyber-capability. The greatest challenge is for technologies implemented from five to 20 years ago. With the shift to AMR and then to AMI, networks and devices continued to get smarter, but there was not much thought given to security. So, this legacy era is the most exposed in terms of cyberthreats.

The second issue involves manpower and budget limitations. Although there are large utility entities that have the capability to address cybersecurity with a full arsenal, many utilities are smaller and fall short on expertise, manpower and time required for system security capabilities. In addition, there may be no security patches available for older systems, and an upgrade of network or devices can be cost- and time-prohibitive.

Another deficiency faced by many utilities is a simple matter of not wanting to break something that works. While the meters and networks work fine without security measures, apprehension about the complexity of encryption and other security measures scares away many utilities from taking action. There is anxiety about breaking the meters, fear of losing meter keys and general apprehension about understanding and using the security measures.

Best practices

Despite the potential trepidation about implementing cybersecurity measures in the current utility marketplace, doing so is truly imperative. Here are some of the approaches electric utilities can take to help ensure their customers—and their businesses—stay safe from today's growing threats.

End-to-end security

This approach considers the weakest link in the systems and is assessed from device to base stations to the network—and ultimately the head-end systems. Security effectiveness involves continuous monitoring and support of devices, as well as regular security patches for customers. It is a truly broad-based "security in depth" look at implementing cybersecurity measures from encryption and malware protection to network security and spectrum protection.

Risk-based, or layered, defense

This tactic addresses high-value assets and implements more control and greater security at those levels. For example, AMI would get a higher level of protection than AMR systems. Moreover, head-end and base-station security takes precedence over meters. If a hacker gets into a single meter, the outcome may be bad—but it's not as detrimental as a head-end attack, where the hacker could potentially impact thousands of customers.

Built-in security

This level of cybersecurity builds safety controls right into the products. For additional threat prevention, utility products must "play well with others" when it comes to third-party-supplied security products, such as antiviruses and firewalls. This way, industry-standard measures and services can be layered with encryption and protection aspects built in to the devices.

Vetting and training

Ideally, utilities should undergo an internal risk-based analysis to determine the best practices for their systems. Then they can establish internal capabilities and actions and apply appropriate security controls. For supply chain security, it is imperative that all partners are themselves prepared against cyberattacks as not to put the utility system at risk. And third-party security certifications, industry-standard products and NIST-approved measures go a long way to establish and maintain customer confidence. Finally, utility-wide employee vetting and training provide a level of frontline security that should be integral—as it would be with any organization that has access to private consumer information.

"Communication network redundancy and resiliency are vital to maintaining security. (And) a private network can be significantly more secure."

BALU AMBADY
Director of security technologies at Sensus

Network matters

Device-level security is certainly key to diminishing cyberthreats. But it is the utility network that establishes a foundational net of security for utility companies and their consumers. "Communication network redundancy and resiliency are vital to maintaining security," says Ambady. "Moreover, a private network can be significantly more secure, as attackers can't use commonly available tools to get into the network as with other networks that operate on public channels."

The greatest network protection, however, comes in the form of licensed spectrum. This FCC-protected spectrum allows for isolation and security, with less disruption possible by hackers.

A private point-to-multipoint network, by its nature, provides an unmatched standard of resilience and security. Unlike mesh systems where communication goes through multiple devices to get to the collectors, private point-to-multipoint systems have fewer attack points available to hackers. Plus, getting into a single meter in a mesh system means potential access to additional meters.

The next big thing

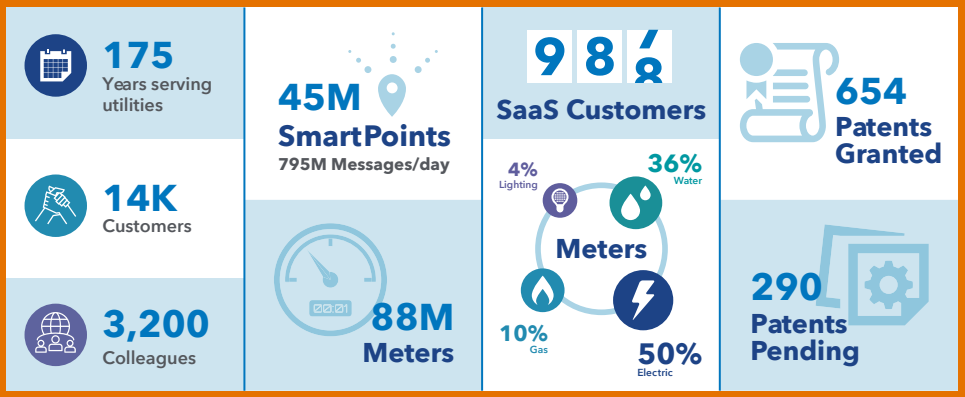
It's important that utilities stay abreast of the latest cybertechnology measures, effectively evaluating these measures and jumping on board with those that are relevant and beneficial. Most recently, advances in cybersecurity that are becoming more prevalent in every industry are blockchain technology and predictive analytics. Blockchain technology stores information across a decentralized, distributed network, making it difficult for a hacker to take down an entire network. "As a sample use case, when you have millions of devices with their own security keys, distributing keys and managing the key lifecycle is challenging," Ambady says. "So within utilities, blockchain technology can help with key distribution. Another new and developing area is to apply data modeling for cyberattack detection."

Grid modernization is changing the way power is distributed and stored, with advances that are benefiting utilities, consumers and communities around the globe. But as staggering IoT innovations continue to be made, the threat of potentially devastating attacks grows as well, mandating that utilities and associated industry partners be vigilant about cybersecurity.

About Sensus

Sensus, a Xylem brand, helps a wide range of public service providers–from utilities and cities to industrial complexes and campuses–do more with their infrastructure to improve quality of life in their communities. We enable our customers to reach farther through the application of technology and data-driven insights that deliver efficiency and responsiveness. We partner with them to anticipate and respond to evolving business needs with innovation in sensing and communications technologies, data analytics and services. Learn more at sensus.com and follow us on Facebook, LinkedIn and Twitter through @sensusglobal.

Sensus by the numbers



SENSUS
a xylem brand

 1-800-638-3748 sensus.com

EVP-10022-02