VIEW POINT

WHY UTILITIES NEED TO MAKE CYBER SECURITY AN URGENT PRIORITY

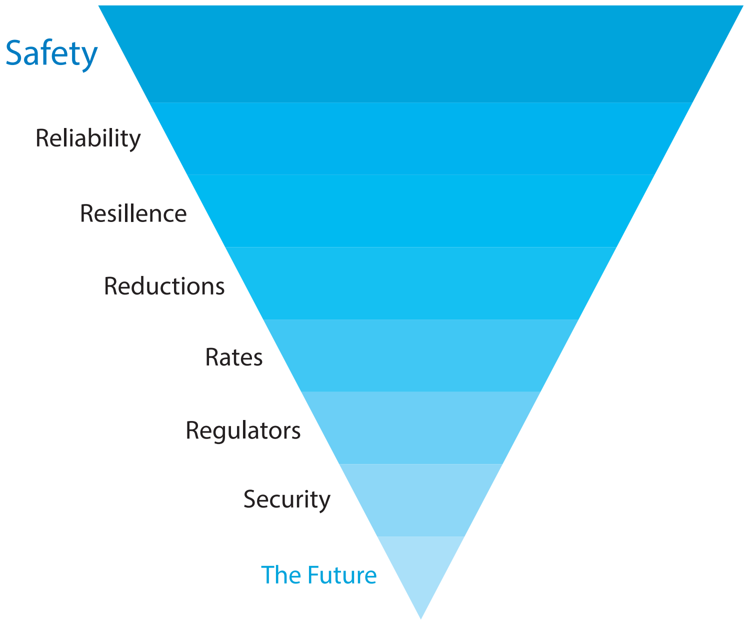
Infosys®
Navigate your next

In the middle of winter’s coldest night in the Midwest, I hear my central heating shut off and jump out of bed to find that the lights are out too. I sit gazing at the dark neighborhood and dropping thermometer, wondering what if the power outage lasts the entire frigid night. I start wondering how my recently installed smart meter might have been hacked to turn off my power, or my online account hacked to send a ‘remote turn-off’ signal, or the grid breached by rogue elements from a rogue state. The Internet is awash with such apocryphal accounts of doomsday scenarios that might not happen today, but are not out of the realm of possibility.

A lot has been done to modernize the smart energy infrastructure since EISA (Energy Independence and Security Act of 2007 or the “Energy Bill”) was enacted to make better use of resources and help the United States become energy independent. EISA 2007 and the resulting research, collaboration, and guidelines by industry bodies such as the NERC-CIP, FERC, NIST standards, and others led to many changes in the industry to keep pace with mandates and modernization demands. However, the rapid convergence of Operational Technology (OT) and Information Technology (IT) network, cloud adoption and distributed energy proliferation in utilities present unprecedented challenges to realizing the vision of the smart grid.

A report commissioned by Infosys in 2018 titled ‘Digital Outlook for Utilities Industry’, found that 66 percent utilities have security as their highest priority. (graph below). While a Global Professional Service Company found that 49 percent of CEOs in the utility industry “say that becoming a victim of a cyber-attack is now a case of ‘when’, and not ‘if’”. This concern persists not only for the critical grid control systems infrastructure, but also for personally identifiable information (PII) of millions of customers that could be compromised by a security breach.

Sequence of priorities for a utility business -
Safety and reliable operations take the top spot



What Can Utilities do to Successfully Fend off a Cybersecurity Attack?

From my extensive interaction with the industry, I believe the first step in implementing a cybersecurity solution is to identify areas where infrastructure might cave in and strengthen these.

- **Integrate OT and IT with a superior security approach**

  Two areas within utilities that are vulnerable to external attack are Operational Technology (OT) systems and Information Technology (IT) systems.

  In OT areas of the grid, industrial control systems, supervisory control and data acquisition devices, and allied technologies used in plants, pipelines, terminals, and rigs have been found to be vulnerable to cyber-attacks. To address this scenario, utilities need to make the right investments, strengthen the security ecosystem, and push for more robust standards from suppliers. A superior resiliency-oriented security approach should encompass physical and data security including privacy.

- **Adopt a careful and security focused cloud strategy**

  As utilities transition to cloud for agility, their cybersecurity teams will need to view this platform through a new lens, and adopt robust, scalable solutions such as cloud access security brokers, and architectures that handle applications and data separately. The focus on vulnerability assessments and cybersecurity risk assessment should reflect in IT operations strategy as well as project solution methodologies.

- **Balance customer trust versus monetization opportunities**

  Personally identifiable information (PII) including usage data will increasingly offer a much needed opportunity for monetization. This could be squandered away even before it materializes, if utilities do not adopt the highest levels of data privacy. More so, as, the risk of attack is only escalating, punitive costs are rocketing and awareness of data privacy through regulations such as GDPR is increasing.

- **Adopt Blockchain**

  While peer-to-peer energy trading was the initial target for blockchain pilots, this 'buzzword technology paradigm' could well be the answer to pressing concerns around personal data from smart meters, billing and financial data or supply chain traceability that is geared towards the security and reliability of the grid. Whether it is pilots led by various power and energy companies like Vattenfall and Innogy in Europe or US based academia/industry partnerships such as energy startup incubator Ameren Accelerator, utilities can benefit from early partnerships to explore the use of blockchain and strengthen safety, security and reliability of the energy grid.

With the cost of a cyber-intrusion running into millions, an innovation partner can ensure the adoption of the right cybersecurity strategy

While utilities try to implement network access controls, protocol-aware security layers, encryption measures, device connection controls, and other integrity measures, comprehensive awareness and personnel readiness remain a challenge. Cybersecurity could be further impaired by poor institutional cyber hygiene such as weak or no password usage, outdated/unpatched software, or poor physical security. All this, even as attack vectors evolve better social engineering tools rather than attacking hardware directly. It is here that an innovation partner acquainted with these complex levers of digital transformation can play the differentiating role between successfully warding off an attack or succumbing to its ravaging effects.

Learn more about how Infosys has helped enterprises address the risk of cyber attacks

- Cyber security services – Run the business, not the risk
- How does an organization cope when a global malware attack paralyses its systems, and its business?
- New cyber security for the new digital enterprise
- Transforming grid operations with digital solutions

About the author

Kapil Nanchahal

Associate Vice President, Resources and Utilities, Infosys

Kapil Nanchahal, heads the new accounts for Utilities, managing the growth and management of new relationships in the Utilities Industry in North America and Latin America. He is an Industry Leader focusing on advising enterprise clients on IT and Business Transformation.

Kapil specializes in IT Enterprise Application strategy and implementation across the value chain of Utilities industry. His experience spans business strategy, growth of new service lines, large transformation initiatives, sales operations and sponsorship of top global alliance partnerships.

For more information, contact askus@infosys.com

Infosys®
Navigate your next