IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

Can IoT Adopters Manage the Security and Privacy Challenges in Smart Utilities?

Phil Beecher

Phil Beecher
President and CEO
Wi-SUN Alliance

Biography

Phil Beecher is President and CEO of Wi-SUN Alliance (https://wi-sun.org/), an industry alliance which promotes standards-based interoperable wireless communications products for smart city and IoT applications, and implements a rigorous testing and certification program to achieve its aims.

With his extensive experience in wireless communications protocols, standards and testing Phil was chairman of IEEE 802.15 TG4g, vice chairman of IEEE 802.15 TG4m (TV Whitespace), vice chairman of the WiFi Alliance Smart Grid Task Group, Chairman of OpenSG Edge Conformity Task Group, Contributing Editor to IEEE802.15.4-2006 and has held positions in the Telecom Industry Association and Bluetooth SIG.

Phil blogs at https://wi-sun.org/blog/

Keywords Internet of Things (IoT), Industrial Internet of Things (IIoT), security, data privacy, smart utilities, research
Paper type Research

Abstract

The utility sector is undergoing a huge transformation, becoming highly connected infrastructures, with millions of endpoints, including smart meters and smart grid devices. These increasingly interconnected systems are a high-profile target for attackers and nation states looking to bring down a country's critical infrastructure. The damaging effects of a data breach or ransomware attack can be devasting, impacting supplies, affecting customers, and damaging a company's reputation. The General Accounting Office (GAO) recently noted that, "nations and criminal groups pose the most significant cyber threats to U.S. critical infrastructure."

Energy security as a whole is a serious concern, not just because of the risk of cyber-attacks, but also because of major economic and geopolitical turmoil, such as the war in Ukraine. But according to research commissioned by Wi-SUN Alliance among senior professionals in the industry, it is also one of the most exciting areas of smart utility development right now.

In this article, the author draws on this research and on Wi-SUN Alliance's Journey to IoT Maturity report published last year to discuss security and whether it can go hand in hand with smart utility development, and looks at energy security in the context of the current economic and political climate, cybersecurity, and data privacy.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Introduction

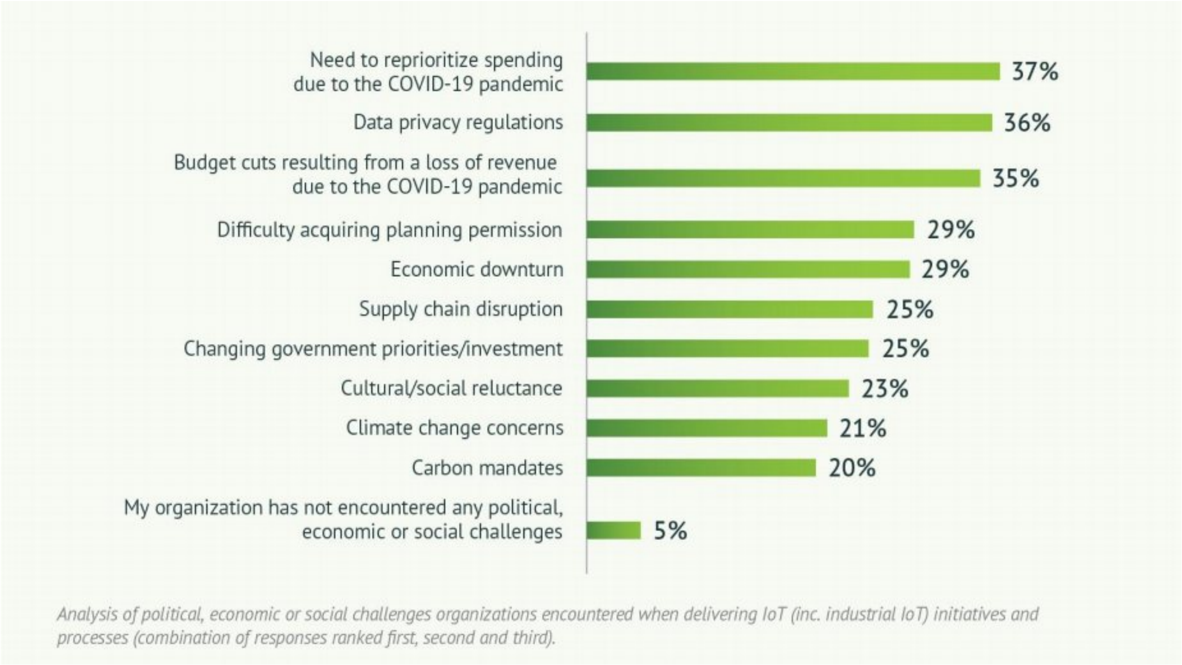
As IoT adoption grows across industries including energy and utilities, so has the development of data-driven technologies for organizations through the Internet of Things (IoT) and, the Industrial Internet of Things (IIOT). The COVID-19 pandemic has accelerated these developments across industries, with many actively embracing IoT technologies, from air quality monitoring sensors to IoT-connected devices in healthcare.

Wi-SUN Alliance published its first 'state of the nation' IoT report in 2017, followed by a 2022 study of UK and US IoT adopters, *The Journey to IoT Maturity*[1], that provided us with an interesting comparison of attitudes among those implementing smart cities, smart utilities and IIoT projects.

What we are seeing is growth in an understanding of what the IoT can deliver. Early adopters it seems have gained confidence from digital transformation projects that have offered quick wins, and as smart solutions have matured. Companies are more likely to be building on their early successes and evolving towards more ambitious strategies. In addition, respondents feel that having an IoT strategy is a must-have, rather than a nice-to-have.

Plans to roll out initiatives have also evolved in the last five years, with projects around security and surveillance, distribution automation, and advanced meter infrastructure all up on the previous study. While newer initiatives like EV charging and connected streetlighting are taking the technology even further.

Figure 1: Political, economic or social challenges when adopting IoT initiatives and processes



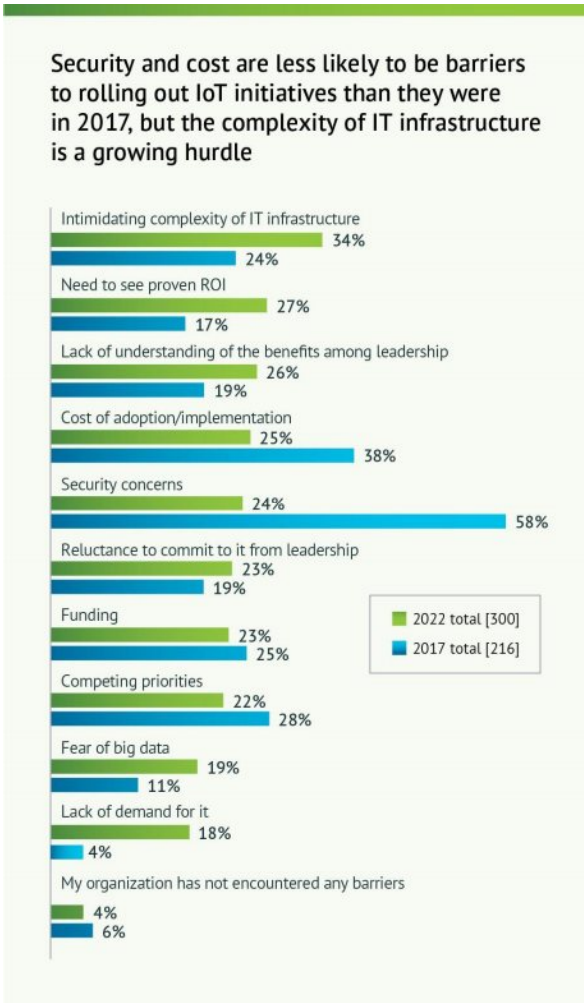
Analysis of political, economic or social challenges organizations encountered when delivering IoT (inc. industrial IoT) initiatives and processes (combination of responses ranked first, second and third).

Source: Wi-SUN Alliance

Security attitudes among IoT adopters

The market is still gaining momentum, with our latest report showing that over 90% of respondents recognize they need to invest more in IoT in the next 12 months to remain competitive as the market continues to evolve. What's more, some initial concerns have also eased in the last five years. For example, IoT adopters ranking security as one of their top three challenges when rolling out IoT fell from 58% in 2017 to 24% in 2022. This change in sentiment is particularly interesting given the current threat landscape.

Figure 2: Barriers to rolling out IoT initiatives



Source: Wi-SUN Alliance

Industry reports suggest that IoT devices are being subjected to a growing number of cyber attacks, such as ransomware and DDoS attacks often for financial gain and theft of confidential data. Such attacks have become particularly prevalent in the energy sector, and more so with the implementation and rollout of smart utilities projects.

It is no surprise that concerns are high among policy makers and governments due to major economic and geopolitical events, including the war in Ukraine putting energy supplies at risk. The U.S. Government Accountability Office (GAO)[2] recently said "nations and criminal groups pose the most significant cyber threats to US critical infrastructure, according to the Director of National Intelligence's 2022 Annual Threat Assessment. These threat actors are increasingly capable of attacking the grid".

With the energy sector facing a growing number of cyber attacks, many of these are aimed at older SCADA systems and increasingly interconnected energy networks, providing plenty of opportunities for threat actors to access systems and disrupt operations. The threat environment right now firmly puts the spotlight on the need to protect critical infrastructure, and the smart networks that utility networks are increasingly reliant upon.

In a Wi-SUN Alliance poll[3] of senior professionals at US utility companies earlier this year, more than three-quarters of respondents said that energy security will be among the most exciting smart/IoT technology developments over the next 12 months. More exciting even than the development of smart buildings and infrastructure, weather and climate related solutions, and disaster management systems.

Data privacy concerns

Looking at attitudes to IoT security in our IoT reports, both progress and optimism come through. But, concerns around data privacy appear to be growing. In our 2022 study, data privacy regulation was the second highest (political, economic, or social) challenge, with more than a third of respondents (36%) placing it in their top three.

Concerns surrounding big data have also increased over the last few years, with almost a fifth of respondents (up from 11% in 2017) placing it in their top three IoT rollout challenges. Many IoT initiatives, from smart metering to smart city projects like streetlighting and transport and traffic management systems, rely on very large quantities of data. While this information may be captured and stored securely, challenges still remain.

A number of new pieces of legislation have come into force since our first IoT report was published in 2017 possibly driving up these concerns, including the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and other privacy regulations. But with stricter data protection laws comes more pressure for city developers, services providers and others to protect sensitive and confidential information – and understand the consequences should they fail to do so.

Managing large volumes of data is challenging and technically difficult, particularly when regulators interpret the data used by many IoT systems as sensitive personal information. Anyone that fails to do, runs the risk of compliance issues that can result in financial penalties and reputational damage.

The momentum behind these smart utilities and smart city projects is exciting and rewarding. But as we see more IoT implementations, ensuring security and data privacy is core to their design and development will be paramount.

Reference

[1] Wi-SUN Alliance (2022) *State of the Nation Report: The Journey to IoT Maturity*. Available at: https://wi-sun.org/iot-maturity-model/

[2] US Government Accountability Office (12 October 2022) 'Securing the U.S. Electricity Grid from Cyberattacks' (12 October 2022). Available at: https://www.gao.gov/blog/securing-u.s.-electricity-grid-cyberattacks

[3] Wi-SUN Alliance (13 March 2023) 'Energy security is most exciting area of IoT technology development, according to Wi-SUN Alliance Smart Utilities Survey'. Available at: https://wi-sun.org/news/energy-security-iot/