Data Privacy for the Smart Grid

The smart grid is defined in Data Privacy for the Smart Grid as “the modernization of electric, natural gas and water grid infrastructure…the convergence of remote monitoring and control technologies with communications technologies, renewables generation, and analytics capabilities so that previously noncommunicative infrastructures like electricity grids can provide time-sensitive status updates and deliver situation awareness.” The majority of people live and work in buildings that use electricity, natural gas and water, and chances are these commodities are delivered via an infrastructure that is slowly becoming smart. The electrical grid is starting to collect information such as where there are power draws, who is pulling the resources, the times that more resources are pulled and perhaps even the types of machines that are pulling these resources. The smart grid facilitates bringing power to people, and the power of the information now captured is part of this transaction.

While this grid is getting smart, it has been a long time coming. This book explains that there have not been any significant, industrywide technology migration initiatives until the smart grid, and the infrastructure is aging. This slow development shows how quickly the industry as a whole has moved in the past to embrace new capital/technology improvements, and this reveals some of the challenges preventing smart grid technology from being installed.

The smart grid is relevant to all those who are interested in data privacy. The more smart devices attached to the grid, the more information is collected on the consumer and about the consumer’s behavior. The book explains that the detailed data collected by the smart grid could allow for forecasts about the number of individuals at a premise, when the location is occupied, sleep schedules and work schedules. The data privacy concerns raised by the authors are numerous and include being able to make assumptions about the health of the residents, which might be of interest to insurance companies, employers and media outlets (for public figures). Criminals could use the data captured from the smart grid to determine if targets are at home and what their routines are, resulting in criminals’ ability to effectively target homes.

This book not only outlines the technology and the possible risk, it also walks readers through risk mitigation methods and how to address privacy. What the consumer needs to know and questions to ask potential service providers to ensure that privacy needs are met are also covered in this book. The authors of this book explain effective information security controls in a simple manner so that when controls are presented to consumers by a company, consumers can assess and evaluate which risk factors are covered by these controls and which may remain.

This book can be used to help informed energy consumers start asking and pushing utility suppliers and regulators to enforce upgrades to the grid now and create regulations upfront to better protect privacy. This book empowers the reader to ask better questions and get better service.

EDITOR’S NOTE
Data Privacy for the Smart Grid is available from the ISACA® Bookstore. For information, visit www.isaca.org/bookstore, email bookstore@isaca.org or telephone +1.847.660.5650.

ENDNOTES
1 Herold, R.; C. Hertzog; Data Privacy for the Smart Grid, CRC Press, USA, 2015

Reviewed by A. Krista Kivisild, CISA, CA, CPA, who has had a diverse career in audit while working in government, private companies and public organizations. Kivisild has experience in IT audit, governance, compliance/ regulatory auditing, value-for-money auditing and operational auditing. She has served as a volunteer instructor training not-for-profit boards on board governance concepts; has worked with the Alberta (Canada) Government Board Development Program; has served as the membership director and CISA director for the ISACA Winnipeg (Manitoba, Canada) Chapter; and is a member of the ISACA Publications Subcommittee. Her areas of expertise are cybersecurity, governance and incident command system/supervisory control and data acquisition systems.

Do you have something to say about this article?
Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article and choose the Comments tab to share your thoughts.

Go directly to the article: