Assessing the value of cybersecurity and data protection in the electricity sector: a choice experiment approach in the Italian context

Proposal for

S51 - Inequality and Territorial Cohesion in the Energy Transition: Towards Fair and Inclusive Low-Carbon Pathways

Elena Ragazzi [a] elenamaria.ragazzi@cnr.it (correspondent)
Ugo Finardi [a], **Jeanne Vallette d'Osia** [a, c], **Graziano Abrate** [b], **Clementina** Bruno [b], Fabrizio Erbetta[b]
[a] CNR-IRCrES, Consiglio Nazionale delle Ricerche – Istituto di Ricerca sulla Crescita Economica Sostenibile, Strada delle Cacce 73, 10135 Torino, Italia
[b] University of Piemonte Orientale – Department of Economic and Business Studies, Via Perrone 18, 28100 Novara, Italia
[c] University of Turin, Lungodora Siena, 100, 10153, Torino, Italy

Abstract

Energy systems, such as electric power networks, are increasingly digitalized. In consequence of this fact makes the concern for cybersecurity is constantly growing. The implications of cybersecurity, data protection and digital sovereignty are many: economic, political and social. Aim of this work is to investigate the economic value of cybersecurity, and in particular its spatial implications, through an apt methodology that takes in account its specific features. From the methodological point of view this work relies on a choice experiment: choice experiments belong to the general group of Cost-benefit analysis methodologies, and more in specific to Stated preferences methodologies. The present one is based on a wide Italian sample of 770 respondents. The sample is balanced in terms of age and geographical macro area. Besides questions investigating the socio-economic and demographic features of the interviewees' households, two sections contain the core part of the survey. The first one of the two presents to each interviewee four scenarios inquiring the will for monetary compensation in change for a blackout of a defined length of time that may incur. In turn, the second one presents to each interviewee three scenarios,

relative to the choice of receiving a monetary compensation in change for a data theft of different gravity. The obtained data have been analysed with the aid of an econometric analysis following a utility function approach. Acceptance rates vary strongly between the different scenarios. High acceptance rates are obviously related to the combination of highest compensation and the lowest level of disturbance in terms of blackout or data theft. In general respondents are sensibly less willing to accept a data theft scenario with respect to the case of a blackout. Coming to the econometric analysis, in the simplified model the only statistically significant variable is the age of respondents. Amore refined model introduces regional characteristics variables. In this case black out data show that geographic peculiarities do not influence significantly the attitude towards the risk of blackout, notwithstanding the Italian regional characteristics. Generation divide is the only relative gap emerging from survey data. Regarding data theft scenarios, the variables that play a strongly significant effect are those measuring previous internet use and data theft experience.

1. Introduction

In a liberalized market, the security of power supply requires effective regulation (Rodilla &Battle, 2012). Moreover, in recent years, the attention of policymakers and researchers has increasingly shifted towards the topic of cybersecurity, which has become a relevant concern from either social, economic and political perspectives (Dunn Cavelty &Wenger, 2020). Indeed, the electricity system is an example of sector where the risk of cybersecurity manifest significantly, with several interconnected infrastructures which are critical to economic development.

First, electrical grids are highly interconnected, and an event occurring locally may easily have wider consequences elsewhere. Moreover, companies that sell electricity possess their customers' personal data, which can lead to specific economic challenges relevant to cybersecurity. Measuring the value of (cyber)security is however a complex challenge, since cybersecurity is not a good traded on the market at a price. Cybersecurity is embedded in electricity provision, ensuring not just delivery but also protection from cyber threats. Since consumers are often unaware of its presence and unable to assign it an economic value, indirect methods are needed to reveal preferences and estimate its worth.

Building on these premises, this paper aims at measuring the value of cybersecurity in the electricity sector integrating two different but complementary perspective: avoidance of service interruption (blackouts) and data protection (avoidance of data theft). Using a choice experiment, we collect data on a sample of 770 Italian individuals, stratified in terms of age and geographical area, using the Qualtrics survey platform. Such dataset not only allows to estimate an average value of security, but also enables to investigate whether such value may be affected by individual, household, and territorial characteristics.

Results suggest that the perceived value of data protection is higher than the perceived value of avoiding power outages.

5. Preliminary conclusions

Estimating the value of (cyber)security in the context of an essential service like electricity supply remains a particularly complex challenge. As cybersecurity is not a stand-alone good traded on the market, its value cannot be directly observed or easily measured through conventional economic approaches. Consumers recognize its importance, yet lack the awareness or technical understanding to assign it an explicit economic value.

Previous literature about electricity security is relatively rich when it comes to the measurement of the value of avoiding a power outage, while the results are usually contingent on temporal and geographical factors (e.g. Carlsson et al., 2021). At the same time, the effects of a cyber-attack may not limit to the interruption in the use of electricity, but can extend to other interconnected infrastructures (Vennemo et al., 2022) as well as to the violation of personal data managed by the electricity providers. This paper contributes to this field of literature estimating the value of cybersecurity in the electricity sector from two complementary perspectives: the avoidance of service interruption (blackouts) and the protection of personal data (avoidance of data theft). Using a choice experiment conducted on a representative sample of 770 Italian individuals, stratified by age and geographical area and administered via the Qualtrics platform, we estimate individual preferences and willingness to accept a compensation for scenarios involving either a blackout or a data theft.

The results indicate that, on average, participants assign a higher value to data protection than to the avoidance of power outages. This finding suggests that citizens are increasingly aware of the risks associated with misuse of personal data, and may consider digital security as a core component of service quality in the energy sector. Moreover, the unique dataset allows to investigate the way the estimated value of security may depend on several individual, household and regional characteristics. As to the protection from blackout, age is a significant factor, with older individuals placing greater importance on

it. In the case of personal data protection, interestingly, individuals who already experienced a data theft is more willing to accept compensation. This might suggest that, at least partially, the individual preferences are affected by the fear of the unknown.

The authors are aware of several limitations. First, some econometric analyses are still preliminary and need to be refined. Second, the study involves only one country (Italy), although with the possibility to investigate widely heterogeneous territories with the country itself. Future studies may include additional countries and compare the results. Another potential limit is that, while in the context of blackout scenarios the levels of proposed discount have proven to be polarize the preferences, in the case of data thief an increase in the upper limit of discount may have resulted in better estimates.

References

Abrate, G., Bruno, C., Erbetta, F., Fraquelli, G., & Lorite-Espejo, A. (2016). A choice experiment on the willingness of households to accept power outages. Utilities Policy, 43, 151-164.

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing cybersecurity as public good: the role of governments, businesses, and individuals. Journal of Legal, Ethical and Regulatory Issues, 16(1), pp. 7-14.).

Black, P. E., Scarfone, K., & Souppaya, M. (2008). Cyber security metrics and measures. Wiley Handbook of Science and Technology for Homeland Security, 1-15.

Boardman, A. E., Greenberg, D. H., Vining, A. R., & Weimer, D. L. (2018). Cost-Benefit Analysis : Concepts and Practice (5th ed.). Cambridge University Press.

Blythe, J. M., Johnson, S. D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Science, 9(1), 1.

Carlsson, F., Martinsson, P. (2008). Does it matter when a power outage Occurs? A choice experiment study on the willingness to pay to avoid power outages. Energy Economics 30, 1232-1245.

Carlsson, F., Kataria, M., Lampi, E., & Martinsson, P. (2021). Past and present outage costs – A follow-up study of households' willingness to pay to avoid power outages. Resource and Energy Economics, 64,(101216). https://doi.org/10.1016/j.reseneeco.2021.101216

Dash, A., Sarmah, S. P., Tiwari, M. K., Jena, S. K., & Glock, C. H. (2024). Cybersecurity investments in supply chains with two-stage risk propagation. Computers & Industrial Engineering, 197, art. 110519. https://doi.org/10.1016/j.cie.2024.110519

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), pp. 5-32. https://doi.org/10.1080/13523260.2019.1678855

Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y., & Cranor, L. F. (2023). Are Consumers Willing to Pay for Security and Privacy of {IoT} Devices?. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 1505-1522).

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. Decision support systems, 86, 13-23.

Hartman, R.S., Doane, M.J., Woo, C.K. (1991). Consumer rationality and the status quo. Quarterly Journal of Economics 106, 141e162.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 3(3–4), pp. 103–117.

Rodilla, P., Battle, C., 2012. Security of electricity supply at the generation level: problem analysis. Energy Policy 40, p. 177-185.

Rowe, B., & Wood, D. (2012). Are home internet users willing to pay ISPs for improvements in cyber security?. In Economics of information security and privacy III (pp. 193-212). New York, NY: Springer New York.

Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). Cybersecurity and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods . Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/24996661.2025.24_00

Vennemo, H., Rosnes, O., & Skulstad, A. (2022). The cost to households of a large electricity outage. *Energy Economics*, *116*, 106394.

Woo, C.K., Ho, T., Shiu, A., Cheng, Y.S., Horowitz, I., Wang, J. (2014). Residential outage cost estimation: Hong Kong. Energy Policy 72, 204-210.

Wooldridge, J.M., 2002. Econometric Analysis of Cross Section and Panel Data. The MIT Press, Cambridge, Massachusetts, London, England