Who is willing to pay for resilience? An evaluation of households' appreciation of the security of electricity system in Italian regions.

Elena Ragazzi, elenamaria.ragazzi@cnr.it (correspondent)
Ugo Finardi, ugo.finardi@cnr.it
Jeanne Vallette D'osia, jeannecharlottemarievallettedosia@cnr.it
CNR-IRCrES, Torino, Italy,

Proposal for the special session 62

A Changing World: Balancing Economic Growth with Sustainable Energy Transitions

Short Abstract

This proposal focuses on cybersecurity as a key element on energy system resilience. The energy transition is deeply transforming the electricity system. This change does not only affect the share of sources and the competitive structure of the market. It has also consequences for the management of the system, introducing new vulnerabilities that may be exploited by cyberattacks. Cybersecurity (CS)regulation is advocated by literature for the electricity sector due to market failure, but lack of information may result in bad regulation.

This paper is focused on the estimation of the value of cybersecurity for citizens, which is important to assess priorities and to avoid overinvestment, with consequences on the cost of energy.

We will adopt a discrete choice experiment approach to elicit the value of CS for respondents who probably do not have competencies nor experience to express directly a value. Results are based on a wide survey on a sample (770 respondents) representative of the Italian population, administered in December 2024.

The survey data-base , which includes also data on the place where the respondent lives, will be complemented with geographical information. Particular attention will be given to the spatial aspects of the problem, both verifying if WTA varies in different geographical data (macro-areas, regions) or types of territories (inner areas, urban vs rural areas). The influence of space-based variables, such as quality of service indicators, malcontent indicators, institutional quality descriptors, will be assessed as well.

Extended Abstract

The energy transition is deeply transforming the electricity system. This change does not only affect the share of sources and the competitive structure of the market. It has also consequences for the management of the system. As is well known, electricity networks have technical characteristics that affect this management; the main one is the necessity to have a real-time balance of electricity injected and consumed. The energy transition is making the structure of the system much more complex respect to the times when electricity was produced and sold through vertically integrated utilities: many different actors, multidirectional flows, new consumption patterns with great variability. Even though the electricity system is designed so as to be resilient even in case of unexpected events, this complexity may cause vulnerabilities, and these vulnerabilities may be exploited by cyber-attackers. Cybersecurity is a continuously changing problem, since menaces are quickly evolving. Cyber attackers update constantly their attacking methodology and, to overcome the system defence, have to exploit situations in which the system is “weak”, such as the imbalances that are often to be afforded in the management of renewables. The increased risks in turn asks for new defenses and generate the need for investments in cybersecurity.

The provision of the good “cybersecurity for the electricity system”, in specific when critical infrastructures are involved, is undermined by several market failures, so literature widely recognizes the importance of regulation or of some public intervention to guarantee such an important service. The perfect allocation of expenses is not necessarily market driven, but it is also difficult to determine from the policy maker’s point of view. Evidence on the value for households to be protected from blackouts caused by a cyberattack or from a violation and exposure of personal data could help their task.

The paper that we will present will be based on a wide survey designed to infer this value from citizens’ preferences.

Since it is difficult to evaluate the value of a good that is not exchanged on a market basis, the research relied on Cost Benefit Analysis (CBA) methodologies aiming at solving these problems. The value of non-market goods can be derived thanks to surveys to a representative sample with ad hoc techniques to assess the Willingness to pay (WTP) an amount of money in order to be able to use a non-commercial good or the Willingness to accept (WTA) an economic compensation in case a good cannot be enjoyed. WTP and WTA can be evaluated through two main types of survey methodologies: the Contingent evaluation, in which direct questions are asked about the WTP and/or WTA for a non-commercial good, or the Discrete Choice Experiment (DCE) approach, in which the respondent is asked to choose between specific scenarios, always involving the good in question. In the specific case of this project, the work involves the use of a choice experiment method to evaluate the value assigned by users of the electricity network to a blackout caused by a cyberattack, through the acceptance of monetary compensation in terms of a discount on the electricity bill, therefore using the WTA as an evaluation tool. The monetary value is assessed through the answer to specific questions related to different scenarios involving the studied problem.

In specific this experiment aims to evaluate the value attached by users to the possibility of incurring in electric power blackouts caused by a cyberattack and the possibility of incurring in a breach of personal data, again due to the activity of cyber hackers.

The interviewee is presented with a set of scenarios relating to a blackout hypothesis that corresponds to a possible economic compensation in the electricity bill. The scenarios can vary by combining duration, time and level of compensation differently. The experimental design involves combining the use of both the within-subject approach (each individual is asked to respond to multiple scenarios) and the between-subject approach (different groups of individuals are proposed different scenarios). In this way it is possible to obtain answers to a wide variety of scenarios without making the questionnaire too long and repetitive (each individual gives his opinion on a limited number of scenarios). The variety of scenarios, with many combinations of duration, time and compensation, is functional to obtain the information to estimate the value attributed to the protection from the cyber-attack that prevents the blackout and modulate this value with respect to the characteristics of the blackout itself. The DCE allows to elicit the value of a good on which the respondent has no direct experience and appreciation. The interviewee faces some hypothetical tough realistic situations and has only to accept or refuse the situation described. The value of the non-traded good is estimated later through econometric models.

The questionnaire included also some questions able to depict the respondent's features, his awareness of the problem, is dependence from service continuity, along with his geographical position. This section of the questionnaire involves questions on the characteristics of the electricity service user: number of people, the standard of living, the average value of the bill, the presence or absence of electrical equipment for which a blackout could be critical, plus a set of questions aimed at

depicting digital literacy. Inequalities in the digitalization of territories and in the digital skills of citizens may affect also the awareness of the importance of investing in cyber-defense and resilience. This information will be used to build variables that can affect the WTA.

Particular attention will be given to the spatial aspects of the problem, both verifying if WTA varies in different geographical data (macro-areas, regions) or types of territories (inner areas, urban vs rural areas). The influence of space-based variables, such as quality of service indicators, malcontent indicators, institutional quality descriptors, will be assessed as well.

We will analyze the results of novel data we collected in December 2024 through a survey. The sample, stratified following the structure of the Italian population, includes 770 valid responses.

Bibliography

Abdullah, S., & Mariel, P. (2010). Choice experiment study on the willingness to pay to improve electricity services. *Energy Policy*, *38*(8), 4570–4581. https://doi.org/10.1016/j.enpol.2010.04.012

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. https://doi.org/10.1016/j.jup.2016.09.004

Al Amosh, H., & Khatib, S. F. A. (2024a). CYBERSECURITY Transparency and Firm Success: Insights From the Australian Landscape. *Australian Economic Papers*, 1467-8454.12385. https://doi.org/10.1111/1467-8454.12385

Algarni, A. M., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems. *Applied Sciences*, *11*(8), 3678. https://doi.org/10.3390/app11083678

Alinsato, A. S. (2015). *Economic Valuation of Electrical Service Reliability for Households' in Developing Country: A Censored Random Coefficient Model Approach*. *5*(1).

Amador, F. J., González, R. M., & Ramos-Real, F. J. (2013). Supplier choice and WTP for electricity attributes in an emerging market: The role of perceived past experience, environmental concern and energy saving behavior. *Energy Economics*, *40*, 953–966. https://doi.org/10.1016/j.eneco.2013.06.007

Amoah, A., Ferrini, S., & Schaafsma, M. (2019). Electricity outages in Ghana: Are contingent valuation estimates valid? *Energy Policy*, *135*, 110996. https://doi.org/10.1016/j.enpol.2019.110996

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), 7-14.*

Aweke, A. T., & Navrud, S. (2022). Valuing energy poverty costs: Household welfare loss from electricity blackouts in developing countries. *Energy Economics*, *109*, 105943. https://doi.org/10.1016/j.eneco.2022.105943

Baik, S., Davis, A. L., & Morgan, M. G. (2018). Assessing the Cost of Large-Scale Power Outages to Residential Customers. *Risk Analysis*, *38*(2), 283–296. https://doi.org/10.1111/risa.12842

Bauer, J. M., & Van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10–11), 706–719. https://doi.org/10.1016/j.telpol.2009.09.001

Bentley, M., Stephenson, A., Toscas, P., & Zhu, Z. (2020). A Multivariate Model to Quantify and Mitigate Cybersecurity Risk. *Risks*, *8*(2), 61. https://doi.org/10.3390/risks8020061

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. https://doi.org/10.1186/s40163-019-0110-3

Boardman, A. E., & Forbes, D. (2011). A Benefit-Cost Analysis of Private and Semi-Private Hospital Rooms. *Journal of Benefit-Cost Analysis*, *2*(1), 1–27. https://doi.org/10.2202/2152-2812.1050

Boxebeld, S. (2024). Ordering effects in discrete choice experiments: A systematic literature review across domains. *Journal of Choice Modelling*, *51*, 100489. https://doi.org/10.1016/j.jocm.2024.100489

Brown, D. P., & Sappington, D. E. M. (2023). Designing Incentive Regulation in the Electricity Sector. *MIT Center for Energy and Environmental Policy Research.*

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, *10*(1), tyae017. https://doi.org/10.1093/cybsec/tyae017

Carlsson, F., Demeke, E., Martinsson, P., & Tesemma, T. (2020). Cost of power outages for manufacturing firms in Ethiopia: A stated preference study. *Energy Economics*, *88*, 104753. https://doi.org/10.1016/j.eneco.2020.104753

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

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Dacus, C., & Yannakogeorgos, P. A. (2016). Designing Cybersecurity into Defense Systems: An Information Economics Approach. *IEEE Security & Privacy*, *14*(3), 44–51. https://doi.org/10.1109/MSP.2016.49

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*, 110519. https://doi.org/10.1016/j.cie.2024.110519

Deutschmann, J. W., Postepska, A., & Sarr, L. (2021). Measuring willingness to pay for reliable electricity: Evidence from Senegal. *World Development*, *138*, 105209. https://doi.org/10.1016/j.worlddev.2020.105209

Entele, B. R., & Ayalew, S. (2024). The cost of electricity interruption for manufacturing firms in Ethiopia: Valuing outage by applying stated preference approach. *Journal of Applied Economics*, *27*(1), 2394715. https://doi.org/10.1080/15140326.2024.2394715

Franco, M. F., Künzler, F., Assen, J. von der, Feng, C., & Stiller, B. (2023). *RCVaR: An Economic Approach to Estimate Cyberattacks Costs using Data from Industry Reports* (arXiv:2307.11140). arXiv. https://doi.org/10.48550/arXiv.2307.11140

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223–240. https://doi.org/10.1108/SCM-10-2018-0357

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, tyv011. https://doi.org/10.1093/cybsec/tyv011

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005

Gorman, W., & Callaway, D. (2024). Do notifications affect households' willingness to pay to avoid power outages? Evidence from an experimental stated-preference survey in California. *The Electricity Journal*, *37*(3), 107385. https://doi.org/10.1016/j.tej.2024.107385

Grutters, J. P. C., Kessels, A. G. H., Dirksen, C. D., Van Helvoort-Postulart, D., Anteunis, L. J. C., & Joore, M. A. (2008). Willingness to Accept versus Willingness to Pay in a Discrete Choice Experiment. *Value in Health*, *11*(7), 1110–1119. https://doi.org/10.1111/j.1524-4733.2008.00340.x

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

Hashemi, M. (2021). The economic value of unsupplied electricity: Evidence from Nepal. *Energy Economics*, *95*, 105124. https://doi.org/10.1016/j.eneco.2021.105124

Hensher, D. A., Shore, N., & Train, K. (2014). Willingness to pay for residential electricity supply quality and reliability. *Applied Energy*, *115*, 280–292. https://doi.org/10.1016/j.apenergy.2013.11.007

Jones, J. A. (2006). An Introduction to Factor Analysis of Information Risk (FAIR). Norwich University Journal of Information Assurance (NUJIA), 2(1).

Kayode, A. B., & Ajoke, A. O. (2016). *Cost-Benefit Analysis of Cyber-Security Systems*.

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability*, *13*(24), 13677. https://doi.org/10.3390/su132413677

Kianpour, M., Kowalski, S. J., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, *116*, 102493. https://doi.org/10.1016/j.simpat.2022.102493

Kim, K., Nam, H., & Cho, Y. (2015). Estimation of the inconvenience cost of a rolling blackout in the residential sector: The case of South Korea. *Energy Policy*, *76*, 76–86. https://doi.org/10.1016/j.enpol.2014.10.020

Küfeoğlu, S., & Lehtonen, M. (2015). Interruption costs of service sector electricity customers, a hybrid approach. *International Journal of Electrical Power & Energy Systems*, *64*, 588–595. https://doi.org/10.1016/j.ijepes.2014.07.046

Kure, H. I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems: Theory & Applications*, *4*(4), 332–340. https://doi.org/10.1049/iet-cps.2018.5079

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Leszczyna, R. (2019). *Cybersecurity in the Electricity Sector: Managing Critical Infrastructure*. Springer International Publishing. https://doi.org/10.1007/978-3-030-19538-0

Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2023). *Mapping the Empirical Evidence of the GDPR's (In-)Effectiveness: A Systematic Review*. http://dx.doi.org/10.2139/ssrn.4615186

Lis, P., & Mendel, J. (2019). Cyberattacks on Critical Infrastructure: An Economic Perspective. *Economics and Business Review*, *5*(2), 24–47. https://doi.org/10.18559/ebr.2019.2.2

Massacci, F., Ruprai, R., Collinson, M., & Williams, J. (2016). Economic Impacts of Rules-versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers. *IEEE Security & Privacy*, *14*(3), 52–60. https://doi.org/10.1109/MSP.2016.48

Meles, T. H., Mekonnen, A., Beyene, A. D., Hassen, S., Pattanayak, S. K., Sebsibie, S., Klug, T., & Jeuland, M. (2021). Households' valuation of power outages in major cities of Ethiopia: An application of stated preference methods. *Energy Economics*, *102*, 105527. https://doi.org/10.1016/j.eneco.2021.105527

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

Morrissey, K., Plater, A., & Dean, M. (2018). The cost of electric power outages in the residential sector: A willingness to pay approach. *Applied Energy*, *212*, 141–150. https://doi.org/10.1016/j.apenergy.2017.12.007

Motz, A. (2021). Security of supply and the energy transition: The households' perspective investigated through a discrete choice model with latent classes. *Energy Economics*, *97*, 105179. https://doi.org/10.1016/j.eneco.2021.105179

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for Cybersecurity. *Daedalus*, *140*(4), 70–92. https://doi.org/10.1162/DAED_a_00116

Nagurney, A., & Nagurney, L. S. (2015). A game theory model of cybersecurity investments with information asymmetry. *NETNOMICS: Economic Research and Electronic Networking*, *16*(1–2), 127–148. https://doi.org/10.1007/s11066-015-9094-7

Nguyen, K. D., Rosoff, H., & John, R. S. (2017). Valuing information security from a phishing attack. *Journal of Cybersecurity*, *3*(3), 159–171. https://doi.org/10.1093/cybsec/tyx006

Nkosi, N. P., & Dikgang, J. (2018). Pricing electricity blackouts among South African households. *Journal of Commodity Markets*, *11*, 37–47. https://doi.org/10.1016/j.jcomm.2018.03.001

OECD. (2018). *Cost-Benefit Analysis and the Environment: Further Developments and Policy Use*. OECD. https://doi.org/10.1787/9789264085169-en

OECD. (2019). *Good Governance for Critical Infrastructure Resilience*. OECD. https://doi.org/10.1787/02f0e5a0-en

Oseni, M. O. (2017). Self-Generation and Households' Willingness to Pay for Reliable Electricity Service in Nigeria. *The Energy Journal*, *38*(4), 165–194. https://doi.org/10.5547/01956574.38.4.mose

Osiolo, H. H. (2017). Willingness to pay for improved energy: Evidence from Kenya. *Renewable Energy*, *112*, 104–112. https://doi.org/10.1016/j.renene.2017.05.004

Ozbafli, A., & Jenkins, G. P. (2015). The willingness to pay by households for improved reliability of electricity service in North Cyprus. *Energy Policy*, *87*, 359–369. https://doi.org/10.1016/j.enpol.2015.09.014

Ozbafli, A., & Jenkins, G. P. (2016). Estimating the willingness to pay for reliable electricity supply: A choice experiment study. *Energy Economics*, *56*, 443–452. https://doi.org/10.1016/j.eneco.2016.03.025

Paté-Cornell, M. -Elisabeth, Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis*, *38*(2), 226–241. https://doi.org/10.1111/risa.12844

Paliński, M. (2022). Paying with your data. Privacy tradeoffs in ride-hailing services. Applied Economics Letters, 29(18), 1719–1725. https://doi.org/10.1080/13504851.2021.1959891

Praktiknjo, A. J. (2014). Stated preferences based estimation of power interruption costs in private households: An example from Germany. *Energy*, *76*, 82–90. https://doi.org/10.1016/j.energy.2014.03.089

Ragazzi, E., & Stefanini, A. (2019). *Are security standards for electricity infrastructure a good choice for Europe? Evidence on cost and benefits from two case studies*.

Ragazzi, E., Stefanini, A., Benintendi, D., Finardi, U., & Holstein, D. K. (2020). Evaluating the prudency of cybersecurity investments: Guidelines for Energy Regulators.

Rowe, B., & Wood, D. (2013). Are Home Internet Users Willing to Pay ISPs for Improvements in Cyber Security? In B. Schneier (Ed.), *Economics of Information Security and Privacy III* (pp. 193–212). Springer New York. https://doi.org/10.1007/978-1-4614-1981-5_9

Rulleau, B. (2023). Household preferences for cyber-attack resilient water distribution networks: A latent class analysis of a discrete choice experiment in France. *Water Resources and Economics*, *43*, 100230. https://doi.org/10.1016/j.wre.2023.100230

Taale, F., & Kyeremeh, C. (2016). Households' willingness to pay for reliable electricity services in Ghana. *Renewable and Sustainable Energy Reviews*, *62*, 280–288. https://doi.org/10.1016/j.rser.2016.04.046

Taddeo, M. (2019). Is Cybersecurity a Public Good? *Minds and Machines*, *29*(3), 349–354. https://doi.org/10.1007/s11023-019-09507-5

Tocock, M., Hatton MacDonald, D., & Rose, J. M. (2024). Risk preferences, bill increases and the future reliability of electricity networks in Australia. *Energy Research & Social Science*, *118*, 103763. https://doi.org/10.1016/j.erss.2024.103763

Vennemo, H., Rosnes, O., & Skulstad, A. (2022). The cost to households of a large electricity outage. *Energy Economics*, *116*, 106394. https://doi.org/10.1016/j.eneco.2022.106394

Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*, *89*, 101659. https://doi.org/10.1016/j.cose.2019.101659

Winegar, A. G., & Sunstein, C. R. (2019). How Much Is Data Privacy Worth? A Preliminary Investigation. *Journal of Consumer Policy*, *42*(3), 425–440. https://doi.org/10.1007/s10603-019-09419-y

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. https://doi.org/10.1016/j.enpol.2014.05.002

Wottrich, V. M., Van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003

Xu, S., Yang, Z., Deng, N., & Wang, B. (2024). Residents' willingness to be compensated for power rationing during peak hours based on choice experiment. *Applied Energy*, *367*, 123335. https://doi.org/10.1016/j.apenergy.2024.123335

Yamaguchi, S., Oshima, H., Saso, H., & Aoki, S. (2020). How Do People Value Data Utilization?: An Empirical Analysis Using Contingent Valuation Method in Japan. *Technology in Society*, *62*, 101285. https://doi.org/10.1016/j.techsoc.2020.101285