Chapter 5
An empirical approach to assess the value assigned by individuals to cybersecurity and data protection

JEANNE C.M. VALLETTE D'OSIA, UGO FINARDI, ELENA RAGAZZI

CNR-IRCrES, Consiglio Nazionale delle Ricerche – Istituto di Ricerca sulla Crescita Economica Sostenibile, Strada delle Cacce 73, 10135 Torino, Italia

Corresponding author: jeannecharlottemarievallettedosia@cnr.it

ABSTRACT
Anchoring the literature review carried in the prior chapters of the Quaderno IRCrES *Cybersecurity and data protection in the electricity sector: state-of-the-art of the literature and evaluation methods* to a practical application is a necessary exercise to grasp entirely the challenges previous studies encountered in estimating the value attributed by individuals to cybersecurity within the electric power sector. This chapter presents our experimental activity, which consists of a representative survey based on a discrete choice experiment designed to evaluate the monetary value the Italian population attributes to electricity blackouts and data theft incidents. Specifically, we examine individuals' willingness to accept compensation in exchange for experiencing an electricity outage or a data breach, with scenarios varying by duration of the blackout and severity of the data theft. Some questions addressing cybersecurity risks in the electricity sector were included intentionally to raise awareness of the public on the topic. The chapter details the development of the survey instrument, beginning with a synthesis on the methodological choices made to ensure its validity, followed by a description of the data collection process.

KEYWORDS: discrete choice experiment, willingness-to-accept, cybersecurity, electricity blackout, data theft.

DOI: 10.23760/2499-6661.2025.24_05
ISBN: 978-88-98193-39-4
ISSN (online): 2499-6661

HOW TO CITE
Vallette d'Osia, J.M.C., Finardi, U., & Ragazzi, E. (2025). An empirical approach to assess the value assigned by individuals to cybersecurity and data protection. In 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* (pp. 65-70). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_05

This chapter describes synthetically an experimental activity entailing a discrete choice experiment (DCE) performed with the aim of evaluating the value attached by the Italian population to a blackout and to a data theft. More specifically, also given the speculative nature of this Quaderno, we concentrate, rather than on the experimental results, on the methodological path that led to the survey, describing how and why we collected data. Thus, we describe in the sections below the survey instrument, with a specific focus on the administered scenarios, and the practical outcome of the survey.

1 JUSTIFICATION OF THE ANALYSIS DESIGN IN THE CONTEXT OF STUDYING CYBERSECURITY FOR THE ELECTRICITY SECTOR

In Chapter 4 (Vallette d'Osia, Finardi & Ragazzi, 2025) we reviewed the main reasons for preferring a DCE experiment over a Contingent Valuation method. First, we align with the literature that finds that respondents are not knowledgeable and experienced enough to directly put a price on the disruption of electrical continuity. Since the DCE method does not require respondents to be able to do so, the method better fits the purpose of our research. Second, since we aim to discover changes in the level of attributes of interest (i.e., we examine different durations of the outage and gravity levels of data theft), we need a method that takes this into account, which is precisely the case with DCEs.

The design of our DCE experiment was therefore developed taking into account the challenges that weaken the validity of the method. Boxebeld (2024) reviewed existing literature to highlight the role of ordering effects within DCEs. In our case, with two alternatives (i.e. Yes, I accept the economic compensation associated with the blackout or data theft/No, I prefer to remain without any blackout or data theft) and two attributes (i.e. blackout and discount for the blackout choice experiment, data theft and discount for the data theft Choice experiment), we do not have strong concerns about either the order of alternatives or the order of attributes effects. Similarly, the position bias, related to the "lexicographic behaviour" mechanism is unlikely to be significant in our case because of the low number of attributes and alternatives. Still, we chose to randomize the order of alternatives since it was not difficult to implement.

However, we do note the presence of choice set ordering effects. Indeed, the position of a scenario within the sequence presented to a respondent could have an impact on both the error variance and the probability of choosing the status quo. Three mechanisms are at play: learning effect, cognitive burden and anchoring effect. The *learning effect* occurs as participants become more familiar with the choice setting, leading to better-defined preferences and more consistent decisions over the course of the sequence. Conversely, *cognitive burden* can set in after the completion of multiple scenarios, causing fatigue, loss of focus, and thus an increase in random or irrational choices. Lastly, the *anchoring effect* suggests that respondents' later choices may be influenced by the attribute levels they encountered earlier, introducing a starting point bias.

To overcome these issues, we adopted some mitigating measures. First, we opted for advanced disclosure of the set-up to induce institutional learning and anchoring before the start of the experiment. To do so, we informed respondents about the number of scenarios and the random variation of attribute levels. Secondly, we gave a visual idea of the scenario that respondent would be seeing prior to the start of the choice experiment so that respondents would become familiar with the topic and environment, thus reducing anchoring effects. Thirdly, we randomized the attribute levels[1] and order of scenarios to prevent starting point bias. Finally, we maintained a low number of scenarios shown to respondents (4 to be completed for the blackout choice set, 3 for the data theft one) to reduce the cognitive burden.

To summarize, the validity of a DCE can be compromised by various ordering effects, highlighted in the literature on the topic; consequently, we implemented mitigation measures in

[1] The levels of attributes were randomized, still, we implemented two constraints: respondents could be asked twice about the same amount of discount, but never more than once the same length of blackout/or the same level of data theft.

our survey design to reduce as much as possible the various biases arising from respondents' learning, fatigue, anchoring, or lexicographic behaviours.

Attribute levels were randomized; however, we implemented two constraints: respondents could be asked twice about the same amount of discounting, but never more than once about the same duration of blackout and/or the same level of data theft.

2 THE DATA COLLECTION DESIGN TO ASSESS THE ECONOMIC VALUE OF CYBERSECURITY IN THE ELECTRICITY SECTOR FOR CITIZENS

This section goes details the approach used to collect the data, concretely explaining the survey instrument that was designed for the purpose and the administration method used to carry out the survey.

2.1 The survey instrument

The survey instrument used is a questionnaire containing a series of questions designed to elicit the respondents' "Willingness to accept" combined with a number of additional questions aimed at framing the respondents' characteristics in detail and raising their awareness on the topic. Specifically, the questionnaire contains four types of questions:

- Questions related to respondent characteristics.
- Questions related to household use of electricity.
- Questions related to knowledge and awareness of specific issues.
- The scenarios.

Table **1** at the end of the section presents the details of the questions included in the questionnaire.

The survey was entrusted to a specialized company, Qualtrics™, which ensured the use of a balanced panel and specific quality control methods. In fact, the panel is constituted as follows:

- Gender: males (48 %), females (52 %), natural spillover due to the presence of non-binary respondents.
- Age: 18-34 (30 %); 35-54 (32 %); over 55 (38 %).
- Geographical origin: North (41 %); Central (21 %); South and Islands (38 %).
- Income: < 50K€ (~35%); between 50K€ and 100K€ (~35%); >100 K€ (~30%).
- Education level: graduates (35%); non-graduates (65%).

In addition, the implementation of the questionnaire included a series of quality checks, which allowed for the identification of actions such as the introduction of illogical answers or random strings of characters, duplication of answers, the presence of bots, and the insertion of random answers (such as "Christmas tree" answers in Likert scales or the constant insertion of the same answer). In addition, a check was made on response times: answers that were too quick (the speeding check was measured as half the median time during the test phase) were automatically eliminated, as were questionnaires that were incomplete or had inconsistent combinations of answers (e.g., on location).

2.2 The scenarios

In the main section of the questionnaire, respondents were faced with two choice sets, including a series of scenarios describing:

- a cyberattack on the electrical system, resulting in a general blackout of different duration, referred to as the *blackout choice experiment*.
- a cyberattack on the electrical system, resulting in a data theft of different gravity levels, referred to as the *data theft choice experiment*.

In addition to randomly display scenarios within the choice sets, we randomized the order of the two experiments. In this way, respondents were equally likely to begin with either the data theft or blackout experiment, each with their own scenarios and related questions.

The scenarios were constructed after a careful review of relevant scientific literature to conform as closely as possible to the state of the art for conducting surveys of this type.

Before viewing the scenarios, the respondent was given a brief explanation in which he or she was asked to identify with the situation described in each question. In this way, the respondent had to assess the possible consequences for the household, with reference to domestic life, carefully evaluating the discomfort caused by the interruption and the proposed discount.

In proposing the scenarios, considerable attention was paid to their randomization, again following the dictates of the scientific literature on the subject. Accordingly, the scenarios were proposed completely randomly, so as to decrease cognitive bias on the part of the respondents (Boxebeld, 2024).

The blackout choice experiment:

Other possible contextual elements affecting the value of the blackout (season of the year, time of the day, day of the week) were not considered to keep the scenario complexity low. The respondent was asked four questions, referring to a sudden power outage that occurred at 6 p.m. on a Wednesday evening in October. In each question the duration of the blackout was different; possible durations were 1 minute, 6 hours, 9 hours, 18 hours and 36 hours. For each outage, a discount was proposed in the bill by the power company. The discount was quantified in different amounts: €1, €20, €40, €60, €80, and €100. Discounts and durations were combined, identifying a list of 30 possible scenarios. No respondent could happen to have to evaluate scenarios with the same duration. Unlike duration, discounts could instead be repeated within the four scenarios proposed to each respondent.

Thus, the proposed scenarios were of the type:

The blackout lasts from 18:00 to XX:XX (duration of XX minutes/hours). The proposed discount is Y €.

For each scenario each respondent was then put in front of the option:

- I would accept this interruption, given the proposed discount.
- I would rather have no interruption and no discount.

The data theft choice experiment:

The respondent was asked three questions, referring to a data theft suffered by their electricity supplier. The type of data breach suffered was different in each question, with four different levels of severity. The levels are defined in a cumulative and hierarchical manner, with each subsequent level encompassing the characteristics of the preceding levels while adding an additional dimension.

- 1st level:
  - Personal contact data (personal data, such as telephone number, postal address and email).
- 2nd level:
  - Personal contact data,
  - Consumption profiles (time slots during which electricity is used at home).
- 3rd level:
  - Personal contact data,
  - Consumption profiles,
  - Login credentials (username and password to authenticate the account under which you manage the contract).
- 4th level:
  - Personal contact information,
  - Consumption profiles,

- Login credentials,
- Data related to payment instruments (credit card or checking account) that could be used for money theft.

As for the blackout choice experiment, each breach was associated with a hypothetical discount in the bill as compensation for the inconvenience suffered, which varied in the same amounts, between €1 and €100. Discounts and gravity levels were combined to generate a total of 24 possible scenarios. Each respondent was presented with three scenarios, each featuring a different gravity level, while discounts could be repeated at most two times across the three scenarios.

Thus, the proposed scenarios were of the type:

The data breach results in the theft of X (level of gravity X, with its description). The proposed discount is Y €.

For each scenario each respondent was then put in front of the option:

- I would accept this data infringement, given the proposed discount.
- I would rather have no data infringement and no discount.

In structuring the questionnaires, particular attention was paid to defining the geographic location of respondents. This was done to analyse potential influences from contextual characteristics on responses regarding the perceived value of cybersecurity. The geography of responses, in fact, allows for correlating the collected data with territorial values. These can relate to technical aspects of the electricity service, such as service quality and continuity, but also to broader contextual factors, such as institutional quality, the geography of dissatisfaction, and the level of legality. Special attention should also be given to analysing differences in response profiles between those living in urban, suburban, or rural areas.

Table 1. Reasoned structure of the questionnaire

SURVEY STRUCTURE	**PURPOSE OF THE SECTION**
GENERAL INFORMATION ABOUT RESPONDENTS	
Gender; age; standard of living; marital status; city size of residence; education level; employment.	Control variables to assess the effect of individual characteristics on WTA.
Place of residence: region, province, municipality, postal code.	Questions aimed at geolocating the respondent to evaluate the effect of contextual variables on WTA.
HOUSEHOLD ELECTRICITY USAGE	
Number of people in the household.	Questions aimed at understanding the household's dependence on electricity.
Cost and frequency of electricity bills.	
Use of various types of electrical appliances.	
Presence of children and/or elderly or non-self-sufficient disabled persons in the household.	
KNOWLEDGE AND AWARENESS OF THE ISSUE	
In the past year, have you experienced a power outage/data theft lasting at least one hour?	

Below are some possible inconveniences associated with a blackout/data theft. Indicate which ones you consider the most serious (you can choose up to 5 options).	Awareness of the likelihood and impact of a blackout/data theft can directly influence WTA.
How do you assess the damage caused by a blackout/data theft?	
QUESTIONS ON THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES	
A list of questions is provided to generate a composite indicator of digital literacy.	Digital literacy may influence awareness, which in turn affects WTA.

Source: Own elaboration.

2.3 The survey

The survey was administered via CAWI (Computer-Assisted Web Interviewing) between late November and late December 2024 through the system implemented by Qualtrics™. At the end of the data collection, the sample consisted of 770 respondents, each of whom answered four different scenarios.

All data were carefully classified and prepared for statistical processing. As mentioned in previous sections, appropriate measures were taken to ensure truthful and non-random responses. In addition to the response verification systems implemented by Qualtrics™, answers given excessively quickly were removed, as well as response sets that showed highly irrational behaviour in comparing different combinations of blackout duration and financial compensation.

3 CONCLUSIONS

This chapter outlines the methodological framework and implementation of the DCE survey built to estimate the economic value attributed by Italian citizens to cybersecurity events in the electricity sector, specifically blackouts and data theft. Justification for the use of DCE over alternative methods was provided, along with a detailed discussion of design choices intended to mitigate known biases such as ordering effects, cognitive burden, and anchoring. The survey instrument was rigorously developed, incorporating questions on individual and contextual characteristics, household electricity use, and digital literacy, to ensure a comprehensive understanding of factors influencing willingness to accept compensation for service disruptions. A structured and randomized presentation of scenarios was employed to enhance internal validity, while data collection through a representative sample and quality checks ensured the reliability and robustness of the dataset. Together, these methodological decisions support the credibility of the experiment and contribute to the literature on valuing cybersecurity-related disruptions in critical infrastructures and energy services.

4 BIBLIOGRAPHY

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

Vallette d'Osia, J.C.M., Finardi, U., & Ragazzi, E. (2025) Methods to assess the economic value of cybersecurity. In 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* (pp. 53-62). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_04