International Journal of Information Security
https://doi.org/10.1007/s10207-024-00847-7

REGULAR CONTRIBUTION

Perceptions and dilemmas around cyber-security in a Spanish research center after a cyber-attack

Joaquín Navajas-Adán[1] · Eulàlia Badia-Gelabert[1] · Laura Jiménez-Saurina[1] · Mª Jesús Marijuán-Martín[2] · Rafael Mayo-García[3]

Abstract
Information and Communication Technologies and Internet networks are present in all aspects of social reality and are essential elements in research, development and innovation centers (R&D&I). Cyber-security is crucial for the progress of the research activities developed in these centers, especially given the exponential growth of cyber-attacks and incidents. The present study aims to assess from a socio-technical approach, how a serious cyber-attack on a Spanish research center has affected staff's perceptions of information and communication systems (ICT) security. This study employed a mixed-methods research strategy, combining quantitative and qualitative methods to provide a comprehensive and nuanced understanding of ICT security perceptions among employees. First a quantitative scale was administered to 1,321 employees 3 years before the cyber-attack and 4 months afterward, to measure ICT security perceptions. Then, qualitative techniques (semi-structured interviews, focus groups, and micro-ethnography) were applied to gain a deeper understanding of the arguments underpinning cyber-security at the center after the attack. The results show that the event had an impact on employees' perceptions, increasing the perceived importance of ICT security, with positive behavioral changes noted, but with doubts about their sustainability over time. Also, the need for cyber-security governance was critically contrasted with organizational reality. Finally, the compatibility of science and cyber-security was a central dilemma, which seems to confront antagonistic poles (research and security ICT) and justify the non-compliance with security protocols by part of the staff.

Keywords Cyber-security · Information security · Cyber-culture · Cyber-attack · Socio-technical approach · Mixed methods research

1 Introduction

Information and Communication Technologies (ICT) have become an integral part of today's social life, encompassing various activities such as work, education, leisure, and interactions with government agencies. Even scientific activity, which plays a crucial role in the competitiveness of economies [1, 2], is closely linked to ICT. On one hand, scientific research relies on the use of these technologies to carry out highly sophisticated processes [3, 4]. On the other hand, ICT facilitates collaboration among researchers, scientists, and R&D&I centers, through a networked scientific structure. Scientific activity predominantly occurs within interconnected public organizations that strive to advance knowledge through various forms of research, including basic, applied, and experimental studies [5].

✉ Joaquín Navajas-Adán
joaquin.navajas@ciemat.es

[1] Socio-Technical Research Center, Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT), Universitat Autònoma de Barcelona, Mòdul de Recerca A. Plaça del Coneixement s/n, Bellaterra, Barcelona 08193, Spain

[2] Radioactive Waste Management Unit, Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT), Av. Complutense 40, Madrid 28040, Spain

[3] Technology Department, Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT), Av. Complutense 40, Madrid 28040, Spain

Published online: 04 April 2024

In the context of scientific organizations and communication networks, the significance of cyber-security cannot be underestimated for the effective operation of R&D&I institutions. The research process heavily relies on secure networks to facilitate intricate computations, such as the efficient analysis of vast data volumes, automation, machine learning, and systems modeling [4].

Therefore, cyber-security assumes a critical role in guaranteeing the optimal functioning of the networked scientific structure, fostering collaboration among researchers, R&D&I centers and state-of-the-art technological infrastructures. Security needs to be ever-evolving so as to face the complexity of attacks on information networks. Cyber-threats are borderless menace that affect governments, businesses, and individuals challenging conventional national security methods [6]. Many agencies have been created with the aim to support cyberspace improvement and reliability, as well as to protect society from threats (including the European Network and Information Security Agency - ENISA - or the National Cryptology Center - CCN-CERT - in Spain). These agencies have reported an almost exponential increase in cyber-attacks [7] and their severe impact on productive activities [8]. They have also warned us about potential cyber-attack targets, especially organizations focusing on knowledge generation (R&D&I centers and universities). Specialized reports reveal that attacks on critical education and research infrastructures increased by over 43% last year [9].

From this perspective, this research focuses on understanding the impact of an external cyber-attack on employees' perceptions of their workplace security, information, and communication systems. To do so, a real-world cyber-attack on a R&D&I center was analyzed in a case study. It is important to note that cyber-security is considered an interdisciplinary activity that extends beyond technological aspects. It encompasses resources, processes, human behavior, and structures aimed at safeguarding cyberspace and the systems utilized in its advancement [10]. Before delving into the case study, we bring a socio-technical perspective to the analysis, pointing out some studies that have emphasized the relevance of the human and organizational factor and the importance of cyber-security in R&D&I centers.

2 Background and related work

2.1 Cyber-security from a socio-technical perspective

There are multiple definitions of the concept of cyber-security. This paper considers cyber-security as a factor resulting from the interaction of technological, behavioral, organizational and social factors. Essentially, mitigating cyber-security risk requires the deployment of robust technology solutions, widespread citizen and employee education, and establishing effective policies and regulations at both the company and government level [11].

This comprehensive approach to the cyber-security of information and communication technology systems is explicitly supported by national, European and international agencies, including INCIBE (Spanish Institute of Cyber-security), ENISA (European Union Agency for Cyber-security) and NIST (National Institute of Standards and Technology), and is transposed into the prescriptive and guiding framework on cyber-security (National Security Scheme, NIST Cyber-security Framework and UE Regulatory Framework). This wide concept of the elements comprising organizational cyber-security can even refer to aspects such as the organization's training and operating experience against cyber-security [12].

It should be noted that the term 'cyber-security' encompasses traditional concepts linked to cyber-physical media, such as 'information security', referred to the physical safeguarding of digital data [13], or 'ICT security', which broadens the focus to include the protection of systems using information and communication technologies [14]. Similarly, the term 'cyber-culture' has ended up subsuming the original term 'Information security culture' [15].

Therefore, cyber-security should be effective in the case of cybernetic actions aimed at violating ICT security policies and damaging information access or services [16]. Such threats are evolving faster than security teams [17]. The development of information security systems, tools and technologies is not enough to face these threats [18, 19]. The defensive and preventive strategy against cyber-threats should overcome approaches, which are merely technology-centered [20, 21]. Organizations focusing solely on technology without considering human factors are more prone to putting their technology systems at risk [22, 23].

2.2 Organizational cyber-security determinants

Scientific literature has revealed the link between organizational culture, human factors and cyber-security [24]. The cyber-security of an organization can be defined as a set of resources, processes and structures implemented with the aim to protect the organizational cyber-space and online systems from in-house or external malicious networks [10]. Drawing upon an extensive literature review, this section presents insights into the determinants of organizational cyber-security. The findings highlight the importance of organizational policies, resource allocation, management, employee compliance, risk awareness as a determinant of

individual behavior, and education or training in dealing with cyber-threats.

Regarding how organizational policies affect cyber-security, annual ENISA's report [25] argues that badly designed or implemented procedures or policies are behind most cyber-security failures. The development of a formal information security policy is a critical aspect of cyber-security. This policy is more than just a formal documentation of the importance of securing information systems; it is about establishing a 'full-life-cycle' strategy for cyber-security. Thus, the policy must be based on a specific risk assessment, supported by management in terms of resource allocation, and communicated to the workforce through training and risk awareness programs [26]. Internal policies and procedures are important not only as safeguards but also for dealing with attacks. A qualitative study of critical infrastructure experts emphasizes the significance of having established policies and procedures to guide incident response and recovery actions [27]. Furthermore, a review of 43 incidents published as case studies in academic journals, reveals that a solid cyber-security policy is critical to protect against cyber-threats, as even the most sophisticated technology is vulnerable without proper policy and governance [28].

Research in policy development has extensively explored how well employees follow established policies. Such policies typically outline employee roles and responsibilities in protecting organizational resources. Crucially, employee compliance hinges on their perception of the information security policy itself [29]. Numerous studies, primarily adopting quantitative methodologies, have sought to identify factors influencing the degree of individual policy compliance, covering a wide spectrum of variables ranging from psychological factors to organizational dynamics. From a psychological perspective, policy compliance has been linked to self-confidence, shedding light on various cyber-security risk behaviors [30]. Additionally, the level of motivation and job satisfaction has been identified as potential moderators in the relationship between organizational norms and behavioral intentions towards compliance [31]. The coercive approach appears to be an undesirable model for encouraging compliance with policies. In this sense, enforcing compliance with these policies may trigger undesirable effects [32]. It has been observed that the severity of sanctions for non-compliance with information security policy affects marginally compared to other organizational measures [33], and excessive monitoring does not necessarily lead to better compliance [34]. In fact, a control-based approach can decrease responsibility and voluntary safety behaviors, and may even create resistance to compliance, as opposed to employee identification and co-responsibility [35].

Some authors point out that lack of attention to the organization's information security policies, underestimating risks occurs even after receiving written instructions on security [36]. A global security survey by [37] concluded that around 34% of organizations considered that careless or unguarded employees were the main cyber-security vulnerability. A study shows that when employees know the information security procedures and policies of their company, they are more competent to manage cyber-security tasks [36]. The importance of professional salaries also has an impact on the loss of sensitive data [38].

The successful implementation of information security policies hinges on robust management support, manifested in clear resource allocation and provision. This includes establishing an adequate organizational structure and having the ability to increase resources in response to unforeseen cyber-attacks [27]. In sum, senior management support improves the organization's preparedness (security readiness) and response for cyber-attacks [39].

Another factor for safeguarding digital assets and ensuring effective cyber-security governance is the need of substantial investment in cyber-security [40]. To combat the growing number of cyber-threats, prioritizing investments in cyber-security measures is crucial, encompassing not only advanced technology but also employee training programs and initiatives to raise security awareness [41]. The capabilities of an organization and the severity of the cyber-threat play a significant role in the strategic decision to invest in cyber-security [42]. Moreover, empirical results support the hypothesis that attacks drive investment in cyber-security [43].

The relationship between management factors and cyber-security is well-established, with management widely regarded as a crucial determinant of an organization's security posture [44]. The costs of cyber-attacks are generally high and lead to increased attention to cyber-security by management. They also augment the probability that companies carry out an information security risk assessment with the aim to identify other vulnerabilities after a cyber-attack [28]. Senior management is ultimately responsible for initiatives relating to risk management and cyber-security in their organizations [45]. A case study exploring a combined cyber-attack, consisting of an attempted password breach and a subsequent data exfiltration attempt, highlights the critical role of senior management in managing the emotional stress experienced within the organization [46]. If management focuses mostly on technical factors, other actions needed to ensure long-term cyber-security could be hindered. Consideration should also be given to developing specific training programs for the strategic apex of the organization, with the goal of engaging senior management in cyber-security management [42].

Beyond intentional non-compliance, ensuring that employees use information technology in a secure manner is clearly related to training, qualification and risk awareness [20, 44, 47]. According to Corradini &Nardelli [48], the main measures to prevent cyber-risks in an organization are risk analysis, training and clear in-house communication. Organizational response initiatives are designed to achieve a significant level of awareness of cyber risks among employees [49].

Human action in the organizational and technological sphere stands as an essential element because it is people that develop, manage and use technology [47]. The development of cyber-security training programs is recognized as a fundamental aspect of enhancing organizational resilience against cyber-attacks. The need for clear operational training, such as how to build and run successful anti-phishing training, has become apparent [50]. The development of a training solution to defend against threats such as phishing must take into account both individual and situational factors [51]. Findings from a study utilizing a simulated cyber-attack scenario in a hospital environment highlight the importance of implementing awareness programs specifically targeted towards medical personnel [52]. It should also be noted that some studies reveal the existence of organizations that focus their digital transformation process on technological elements, subsuming cyber-security to a purely technological outcome [3, 53]. Attempts have also been made to parameterize "trust" in human behavior by quantifying predictability of response or decision, reliability or consistency, competence, and degree of responsibility [54].

The qualifications of the staff in the cyber-security field are also needed to detect and make decisions in case of security events [55]. In that regard, Stacey et al. [46] underline that the higher the number of individuals in an organization who are aware and understand the implications of ICT security, the more likely it is for positive and proactive decisions to be made. This illustrates that employees are a key element of cyber-security and that, without their consideration, technical solutions fail [8]. As shown in a report on the cost of data filtration [56], approximately 36% of substantial cyber-security infringements are caused by employees' failure to comply with norms, remote work and a lack of security skills.

Finally, the risk perception of the organizations' members is a common and recurring element in the literature. This perception is directly related to multiple factors, ranging from experience with cyber-attacks to more intangible elements such as the cyber-security culture of a given organization. Paradoxically, reduced reliance on technological elements such as firewall and antivirus software appears to be correlated with heightened risk awareness [57]. Additionally, security experiences, especially when they relate to significant accidents, affect the cyber-risk perception and response effectiveness [58]. In that sense, previous experience of a threat affects the way in which individuals perceive future threats of a similar nature [59, 60]. Notably, a study in a sandbox lab environment for similar real-world cyber-defense scenarios found that team leadership can affect the effectiveness of teams against threats [54].

Within the burgeoning field of cyber-security literature, organizational culture is an increasingly crucial consideration. In a study with European stakeholders from critical sectors (including open banking, supply chain, privacy-preserving identity management, security incident reporting, maritime transport, medical data exchange, and smart cities), cyber-security culture emerged as a significant organizational vulnerability and a common challenge across all industries [61]. Organizational elements such as social pressure and incident reporting practices emerge as key issues for cyber-security within organizations. Whereas, social pressure can significantly influence individual behavior, potentially leading to safe or unsafe cybersecurity practices [62], fostering a culture that encourages open and honest reporting of incidents and anomalies, free from fear of reprisal, can promote organizational learning, allowing organizations to identify and address vulnerabilities [63]. Therefore, to help improve in the face of potential threats, it is important to monitor organizational culture on a regular basis with periodic security assessments [64].

2.3 Cyber-security in public R&D&I centers

Large technological research centers (such as critical infrastructures) are complex socio-technical systems that require holistic strategies that combine the simultaneous orchestration of technical solutions with organizational actions [19]. Leading agencies in the field of cyber-security have issued warnings regarding the exponential rise in cyber-attacks targeting public institutions. The complexity of cyber-attacks and the campaigns used to launch them is increasing [10, 65]. Public sector organizations face inherent challenges in allocating economic resources towards cyber-security solutions and services [66]. While it may be difficult to quantify the economic impact precisely, the consequences can manifest in the form of diminished credibility and a deteriorating public image for the organization, potentially hindering the achievement of their public service goals [67]. However, some authors have projected future cyber-attacks by reviewing the most significant events of the past 20 years. They estimate that in the next 5 years, there will be 1,100 major cyber-attacks on critical infrastructure worldwide, causing damages exceeding one million dollars [68]. Cyber-attacks on hospitals and healthcare centers have been on the

rise and have had the greatest impact since the COVID-19 pandemic [69].

In terms of specific considerations for public organizations certain organizational factors seem especially relevant in terms of cyber-security: the facility's ICT security policy, management support, as well as tools and experience [70]. A factor worth mentioning is senior management's acknowledgment and awareness of cyber-threats as a critical consideration [71]. One of the responsibilities of senior management is to favor the development of a suitable cyber-security culture [72] which contributes to preventing cyber-incidents. Security culture should raise awareness about cyber-risks and workforce skills as pillars of cyber-security. Research carried out by universities [73] has favored the identification of a large list of factors which contribute to a strong organizational culture focused on cyber-security in university centers. Few scientific publications comprehensively address the psychosocial impact of cyber-attacks on critical infrastructure. Following the May 2022 attack on the Irish public health system, a study conducted post-event focus groups to understand organizational resilience to ICT system loss. One of its main findings indicates that the stress caused by the attack outweighed the cumulative effect of the COVID-19 pandemic [74].

In summary, based on the above, R&D&I organizations have complex decision-making processes and generally budgetary constraints that translate into limitations in terms of technical equipment or personnel, while the wealth of data and information they generate tends to make them a prime target for cyber-attacks. However, this organizational specificity does not mean that the foundations of the security of their IT systems are based on differentiated aspects, but rather that elements common to other types of organizations are the key to their cyber-security (among other not insignificant aspects, management commitment, organizational factors and the establishment of a strong organizational culture focused on ICT security).

Within the Spanish R&D&I context, there is a set of facilities, research and services available for state-of-the-art, top-quality technological research and development. These facilities, called Unique Science and Technology Infrastructures (hereinafter USTI), received significant funds for cyber-security, including the deployment of ultra-fast and safe communication networks [75]. These facilities provide access to over five thousand R&D&I projects yearly, employing more than 2,000 people, 80% of whom are scientific and technical personnel [76]. The high value of their research is a priority target for cyber-attacks.

This research is developed at a Spanish Public Research Center assigned to the Ministry of Science and Innovation and includes different USTI. This case study attempts to assess how a relevant cyber-attack on an organization has impacted the perception of risk and security of information systems amongst organization members. It is assumed that cyber-security is the result of interaction between technology, human behavior and organizational factors [10].

Based on this perspective, this study adopts a theoretical model [77] that encompasses four distinct dimensions of ICT security. The model is derived from an extensive literature review, considering that cyber-security (or, as the authors call it, information security culture) inherently has elements of a cultural and organizational nature. It is worth noting that the strength of the model lies in the fact that it shows "the relationship between organizational culture and the ICM (Information Security Management) from a 'practice' perspective" [77]. In other words, the model extends the cyber-security framework by introducing organizational and cultural aspects as elements that contribute to the security of information and communication systems beyond technical factors. The four model's dimensions are: Compliance (which mainly refers to employees' behavioral adherence to policies); Communication (which refers to how an organization communicates policies to individuals and employees' expectations regarding information security); Accountability (which refers to the organization's response to employees' violation of information security policies); and Governance (which refers to the positioning of information security in an organization and also on management's perception of its significance). By integrating human, organizational, and technological viewpoints, this model serves as a valuable framework for understanding the fundamentals of cyber-security in a given organization from a socio-technical perspective. As detailed in the methodology section, the four dimensions were used as the primary thematic axes for conducting a content analysis of qualitative information in relation to the specific objectives of the study.

3 Methodology

3.1 Objectives

The study aims to assess the impact of an external cyber-attack on perception of the security of information and communication systems in a public organization. The research was conducted through a case study in a R&D&I center that had experienced a cyber-attack. Two objectives are pursued by the analysis:

a) To determine the specific aspects in which the cyber-attack affected employee's perception of the ICT security in the R&D&I center.

b) To identify and analyze the main arguments and themes expressed by the members of the organization regarding their perceptions of information security after a cyber-attack.

3.1.1 Description of the case study

The research is developed in the context of a case study in an important research center of Spain that employs about 1,294 people and whose R&D&I activity is carried out nationally and internationally. The average age of the staff is 47.7 years. The center's central campus is in Madrid, with offices scattered around the country. Information and communication technologies in this research center are corporate services managed from the central campus. This center has technological infrastructures that provide support to both research projects and technical and administrative programs.

This research was rolled out after the cyber-attack suffered by this center in January 2022, hampering the access of all employees to the center's ICT services. Given the characteristics of the event and its significant level of severity, it was considered as a serious cyber-attack [78]. Specifically, a Trojan malware was resident in one user's PC and detected by the software cyber-security sentinels installed in all the equipment by the ICT central services following the previously adopted directive from the Computer Emergency Response Team of the National Cryptologic Center (CCN-CERT). In response to the cyber-attack and to mitigate potential effects, the center promptly took measures to safeguard stored information. As a precautionary step, all communication, both internal and external, was immediately canceled. This action aimed to prevent further damage and ensure the preservation of critical data. It should be pinpointed that the detection of the malware forced absolute disconnection from any link outside the Center. Hence, for several weeks there was no Internet, no email, no exchange of data with large collaborations and experiments and no access to IT services. Jointly working with the cyber-security agencies from the National administration, those services were open gradually as additional cyber-security measures were being adopted. The potential severity of the threat to the center's information systems determined the radical nature of these measures, which in themselves had an enormous disruptive capacity to the organization's daily activities. It is worth noting that the perception of the severity of the attack by members at all levels of the organization was based on the impact of these preventive measures, rather than as a direct result of the information hijacking.

Table 1 Research methods

Research Method	Type of Information	Scope
Scale: Perception of ICT security in the work environment	Quantitative Data (Likert scale 1–7)	Entire Organization. There is data available from 2019 (before the cyber-attack and 2022 (after cyber-attack).
Semi-structured interviews	Qualitative Data	Directors and people in charge of information systems. There is data available from 2022 (after cyber-attack).
Focus Groups	Qualitative Data	Focus groups of researchers, support staff, and territorial centers. There is data available from 2022 (after cyber-attack).
Micro-ethnography	Qualitative Data	Personnel from the Department of Information Technologies. There is data available from 2022 (after cyber-attack).

3.2 Research methods

This study was developed according to the principles of the mixed methods research, conceived as "*the class of research where the researcher mixes or combines quantitative and qualitative research techniques, methods, approaches, concepts or language into a single study*" [79]. The complementary use of different types of techniques (qualitative and quantitative) yields deep, valid and reliable knowledge of the research subjects [80]. The application of different research types enhances validity and minimizes subjective interference in the data interpretation process [81]. It also enables using the results of one technique as a reference to move forward with the application of other data collection techniques [82].

The adoption of a mixed methodology in this research is due to two reasons: (a) its direct synergy with a socio-technical approach, which delves into processes within complex systems with different levels of knowledge, and (b) its pragmatic value, i.e. its analytical power to provide knowledge in applied research projects (such as safety culture assessments, where triangulation of information from different techniques provides solid findings).The following table (Table 1) shows the research methods applied.

3.2.1 Scale: "Perception of ICT security in the work environment"

The scale was developed and validated initially in the framework of an organizational and safety culture assessment carried out in 2019. The items were developed according to the

needs of the Information Technology Unit of the Research Center which was in the first stage of adapting technological systems to the National Security Scheme [83]. Specifically, the goal was to determine a measure of employees' perceptions of ICT security as an indicator of their overall level of awareness. The scale was created in a collaborative process between the researchers and the ICT department's technical staff to ensure its face validity. The starting point was to include perceptual items that could provide a global perception of ICT security in the center. It is a shortened scale that does not pretend to cover all organizational aspects related to the perception of ICT security, but whose different items share as a common nexus issues that affect the overall perception of ICT security.

It is important to highlight that the scale used in this study focuses on measuring the subjective perceptions or views of individuals regarding ICT security in their work environment. Thus, the scale consists of 4 items that measure specific aspects that provide an overall perception of ICT security. Respondents were asked to indicate their level of agreement (7-point Likert scale, where 1 is strongly disagree and 7 is strongly agree). Each item and the underlying element of the National Security Scheme (NSS) related with security are shown below (Table 2).

The scale was distributed to staff in the center, onsite and remotely, at two different moments in time:

- Time 1, June & July 2019 (within the framework of a safety culture assessment).
- Time 2, May 2022 (four months after the cyber-attack).

3.2.2 Semi-structured interviews

A total of five one-on-one semi-structured interviews were carried out in 2022 with both the department head and unit heads of the ICT department (Time 2). They were conducted by two researchers, and lasted approximately one hour each. During the interviews, handwritten notes were taken, which were later transcribed for further analysis and interpretation.

The objective of these interviews was threefold: (a) To gain insights into the perspectives of department and unit heads regarding the impact of the cyber-attack and their respective roles and responsibilities within the ICT department. This aimed to understand their unique viewpoints and experiences in relation to the attack; (b) To identify key thematic elements that should be incorporated in the development of a protocol for conducting focus groups. This objective aimed to determine the crucial topics and areas of discussion that would be relevant and informative for conducting focused group sessions related to the cyber-attack; and (c) to create a Behaviorally Anchored Rating Scale (BARS) to narrow down the discussion in terms of ICT security. BARS are categorical instruments that allow to typify (and quantify) organizational behavior are primarily designed for evaluating the performance of specific job roles or positions within a job family [84]. However, from an organizational standpoint, BARS can also serve as a valuable complementary tool to gain insights into perceptions regarding organizational processes and cultural norms [85]. In this study, the BARS were utilized to narrow down the discussion in terms of ICT security. The content of the BARS can be found in Appendix 1.

In short, by accomplishing these objectives, the study aimed to gather comprehensive insights from department and unit heads, develop an effective focus group protocol.

Prior to carrying interviews out, guidelines containing pre-established thematic areas were prepared based on the research goals. The following Table 3 shows the list of interviewees and the thematic questions that were asked.

Table 2 Description of the scale items and the NSS elements to which they relate

Item	NSS elements that make up ICT security perception
1 Emphasis is placed on the necessary precautions to avoid computer attacks.	The organization's cyber-security effort (Higher scores suggest the organization strives to enhance prevention).
2. Personnel is aware of the risks of using ICT applications.	Risk awareness (Higher scores suggest greater sensitivity towards ICT risks)
3. Information security is important in my job.	ICT security significance (Higher scores suggest a greater understanding of the relevance of ICT security amongst respondents).
4. In general, I trust ICT security at the organization.	Confidence in ICT security (Higher scores suggest greater trust in information security).

3.2.3 Focus groups

At Time 2, eight combined focus groups were conducted: face-to-face (four) and online (four), with a total of 26 participants. The combination of face-to-face and online sessions allowed for flexibility and ensured broader participation from individuals involved in the study. The selection of participants for the interviews and focus groups followed the criteria of intentional sampling on a voluntary basis. In addition, groups were put together based on organizational criteria, with the aim to ensure their homogeneity (researchers; support personnel; personnel from different locations).

They were conducted by two researchers and ranged in length from 45 min to 1 h and 15 min. As with the

Table 3 List of interviewees and thematic questions

Interviewees	Thematic questions
ICT Department Manager Computer Application Design Manager Computer Application Design Technician ICT Architecture Manager Scientific computing manager	The impact of the cyber-attack on the center. Organizational response to the cyber-attack (from a technical and organizational perspective). Perception of the ICT department regarding the response of the center's members (at all levels) during the cyber-attack. Changes in the center (at all levels and of all types) as a result of the cyber-attack. Examples. Impact of the cyber-attack on the center's research mission. Identified desires or needs to strengthen the center's ICT security.

Table 4 Focus group abbreviated form protocol

Focus Group protocol
- Welcome and introduction - BARS: ICT Security o Individual qualification. o Sharing and justification. Examples. - Complementary questions for group discussion: o Changes in the organization after the cyber-attack. o ICT security needs. o Impact of ICT security on different kinds work inside organization o Brief definitions of ICT security in the organization.

semi-structured interviews, notes were taken by hand and were subsequently transcribed.

The focus groups were performed on the basis of the protocol developed after the interviews (Table 4). The ICT Security BARS designed were introduced in the focus group with the purpose of contributing to the individual reflection of the participants prior to the group discussion. There was no theoretical reference to conceptual models of cyber-security, and participants were encouraged to be free to express their opinions.

3.2.4 Micro-ethnography

The research included a micro-ethnography process, which consisted of conducting immersive observations in a specific location for a short period of time with the aim of capturing detailed interactions around ICT security processes [86]. The enography lasted 6 working days. A researcher traveled to the center's central campus and set up in the ICT department. This process involved active observation and interaction with members of the center. During these observations, the researcher recorded facts and perceptions, both objective and subjective, in a field diary. This field diary is a concise document that captures stories about local practices and situations. This field diary is an integral part of the textual corpus of this research project, along with the notes from the interviews and focus groups.

Table 5 Survey sample and descriptive

	VARIABLE	2019	2022
Type of activity	Management	12	5
	Research	652	264
	Support	178	96
	Unknown	*35*	*41*
Seniority	from 0 to 5 years	137	77
	from 6 to 10 years	87	23
	from 11 to 20 years	259	126
	from 21 to 30 years	200	56
	more than 30 years	125	99
	Unknown	*69*	*27*
Location	Central campus	586	371
	Territorial centers	89	23
	Unknown	202	50
TOTAL		877	444

A comparative analysis of gender could not be performed because it was not included in the demographic options at time 2.

4 Data analysis

4.1 Sample description

The survey study sample is comprised of 1339 workers from the public research agency above-mentioned. Initially, in 2019, the scale was administered onsite to 895 people within the framework of an organizational culture evaluation at the research center. Later, in 2022, the scale was distributed online to 444 people after the cyber-attack sustained by this agency in January 2022. As for interviews and individual groups, the total sample includes 26 people. More specifically, five individual interviews and eight focus groups (five face-to-face and three remote) were held.

The sociodemographic characteristics associated with the survey (Table 5) are shown below. Due to confidentiality reasons, the name of the center, the names of the departments and the participants' identification are not disclosed.

4.2 Quantitative analysis

All data analyses were conducted using IBM SPSS Statistics v28.0 [87]. The distributions of scores, skewness and kurtosis suggested data were normally distributed.

Construct validity was studied using principal component factor analysis [88, 89]. A factorial solution that explains at least 50% of the total variance is considered adequate [90].

Table 6 Results of factorial analysis

	Total variance explained					
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	2,410	60,261	60,261	2,410	60,261	60,261
2	0.756	18.889	79,149			
3	0.491	12.275	91,425			
4	0.343	8.575	100,000			

Extraction Method: Principal Component Analysis

Cronbach's alpha (α) internal consistency reliability [91] was calculated for the scale, considering acceptable values of α as from 0.7 [92]. Also, it was taken into account that the lower limit of the confidence interval is 0.7 or more, as that would ensure that even in the most unfavorable scenario, score reliability would be acceptable [93].

Student's t-test was used to compare the means of the scales' items considering demographic segmentation and determine if the difference in means is statistically significant. Tests were considered significant at $p < 0.05$.

4.3 Qualitative data analysis

All textual data (interview notes, focus group notes, and micro-ethnographic field diary) were analyzed according to the following analytical process [94]:

a) Data preparation: Textual documents were renamed to remove any confidential or personal information regarding the participants.
b) Coding: A detailed reading was conducted to identify data segments with relevant codes that represent ideas, concepts, or themes related to ICT security.
c) Categorization: In contrast to the usual approach in qualitative analysis, we did not adopt the inductive principles of grounded theory [95]. Instead, we utilized the pre-established categories of the four dimensions proposed by Tang et al. [77]. Therefore, the coded concepts were grouped based on this framework.
d) Interpretation: The interpretation of the qualitative data was guided by the concept of "interpretive repertoire" [96]. This concept refers to how people employ language to understand and shape the meaning of reality. Codes with similar ideas were grouped within each dimension, which were then considered as 'interpretive repertoires' in the context of ICT security.

The analysis process involved the participation of three researchers, who engaged in a collaborative coding-categorizing and questioning process based on the consensus [97].

Table 7 Reliability and descriptive statistics of the scale

Perception of ICT security in the work environment scale				
	M.	SD.	N.	α
2019	4.77	1.19	877	0.77
2022	5.20*	1.12	444	0.72

5 Results

5.1 Quantitative results

5.1.1 Reliabilities, factorial components and global descriptive of the scale

The results of factorial and reliability analyses show that only one component was extracted, which means all scale items are integrated into the same factor. That is, the 4 items in the scale are interrelated with one another and measure the same construct ("Perception of ICT security in the work environment"). That integration, above 60%, is considered adequate (Table 6). In addition, the analysis of the internal consistency of items comprising the scale shows a Cronbach alpha value of 0.77 [95% CI 0.75; 0.80], which is considered acceptable (Table 7).

It is worth mentioning that to interpret results (seven-point Likert scale), the rates established by Pimentel [98] were used.

As shown in Table 7, considering this criterion, the average score on the "Perception of ICT security in the work environment" scale was "good" in both 2019 and 2022 administrations *(2022 M = 5.20; 2019 M = 4.77)*.

The scale "Perception of ICT security in the work environment" scores significantly higher in 2022 than in 2019 *(2022 M = 5.20; 2019 M = 4.77)* (Table 7).

Considering the variable type of activity, there are no statistically significant changes between scores in 2019 and 2022 in the perceptions of personnel involved management activities *(Managers 2022 M = 5.20; Managers 2019 M = 4.50)*. However, the analysis shows that personnel involved in research and support activities scored significantly higher in 2022 compared to 2019 *(Research 2022 M = 5.14; Research 2019 M = 4.79), (Support 2022 M = 5.38; Support 2019 M = 4.79)* (Table 8).

Table 8 Scale average means for type of activity: (a) management, (b) research and (c) support

Perception of ICT security in the work environment			
a) Management			
	M.	SD.	N.
2019	4.50	1.26	12
2022	5.20	0.82	5
Perception of ICT security in the work environment scale			
b) Research			
	M.	SD.	N.
2019	4.79	1.20	652
2022	5.14*	1.14	264
Perception of ICT security in the work environment scale			
c) Support			
	M.	SD.	N.
2019	4.79	1.12	178
2022	5.38*	1.10	96

Table 9 Scale items average means for (a) 0–5, (b) 6–10, (c) 11–20, (d) 21–30 and (e) > 30 seniority

Perception of ICT security in the work environment scale			
(a) 0-5y			
	M.	SD.	N.
2019	4.56	1.13	137
2022	5.27*	1.16	77
Perception of ICT security in the work environment scale			
(b) 6-10y			
	M.	SD.	N.
2019	4.58	1.25	87
2022	5.35*	1.28	23
Perception of ICT security in the work environment scale			
(c) 11-20y			
	M.	SD.	N.
2019	4.76	1.23	259
2022	4.98	1.20	126
Perception of ICT security in the work environment scale			
d) 21-30y			
	M.	SD.	N.
2019	4.87	1.08	200
2022	5.18	1.10	56
Perception of ICT security in the work environment scale			
(e) > 30y			
	M.	SD.	N.
2019	4.94	1.13	125
2022	5.43*	0.95	99

Considering the variable seniority, the analysis shows statistically significant differences between scores in 2019 and 2022 in personnel working in the organization for 0–5 years, 6–10 years and over 30 years *(0–5 years 2022 M = 5.27; 0–5 years 2019 M = 4.56), (6-10y 2022 M = 5.35; 6-10y 2019 M = 4.58), (> 30 years 2022 M = 5.43; >30 years 2019 M = 4.94)* (Table 9).

The analysis by the variable 'location' shows statistically significant differences between scores in 2019 and 2022 in personnel working in the central campus (Central Campus 2022 M = 5.21; Central Campus 2019 M = 4.80) (Table 10).

Table 10 Scale items average means for location

Perception of ICT security in the work environment scale			
Central Campus			
	M.	SD.	N.
2019	4.80	1.19	586
2022	5.21*	1.14	371
Perception of ICT security in the work environment scale			
Territorial Centers			
	M.	SD.	N.
2019	5.12	1.13	89
2022	4.99	1.01	23

*Note: Mean = M.; Standard Deviation = SD.; Sample = N.; Significance = * (Bonferroni – corrected p < 0.05)*

Table 11 Summary of Quantitative Results

- The significant scale variation shows that the, in global terms, the relevance of ICT security in the work environment has significantly increased after the cyber-attack received.
- The analysis by variables shows the following main findings:
  - The perception of ICT security by those involved in management activities has not changed since the cyber-attack. The values remain as high as in time 1.
  - Personnel involved in research and support activities change their perception of ICT security. After the cyber-attack, the importance of ICT security increases significantly.
  - The perception of ICT security of personnel with 11–30 years of seniority (44.61% of 2022 personnel) has not changed since the cyber-attack. However, people under 10 years of seniority (24.51% of 2022 personnel) and over 30 years of seniority (24.26% of 2022 personnel) have significantly increased their perceptions of ICT security.
  - The perception of ICT security of personnel working at the Central Campus (% of 2022 personnel) has changed since the cyber-attack (the importance of ICT security has increased significantly) while people working in Territorial Centers score in the same order of magnitude in 2022 as they did in 2019.

The main quantitative results are shown on Table 11.

5.2 Qualitative data results

The results of the analysis will be presented in a simplified way, grouped according to the dimensions of Tang et al. (2016) and the main interpretative repertoires identified.

5.3 Compliance

It refers to employees' behavioral compliance with information security policies.

It is perceived that the cyber-attack has paradoxically brought about some benefits in this dimension. More specifically, it is perceived that after the cyber-attack, organization members have globally developed safer behaviors. Some of the many examples given to support this statement include one referring to uninstalling external programs and

reducing the use of non-licensed programs. On the opposite, they mention that this is probably a temporary effect which, in time, will lead to "relaxation" and to more frequent non-compliant behaviors once the memory of this event fades over time. A lack of cyber-security regulatory compliance is also cited, linking it to a lack of accurate knowledge of security protocols and work compliance requirements (work completion is considered more important than cyber-security). Table 12 shows the main interpretative repertoires of the 'Compliance' dimension.

5.4 Communication

It refers to how the organization explains its information security policies to employees. It also alludes to the expectation of employees regarding information security.

An analysis of the discourse reveals that the organization's communication policy during the cyber-attack is favorably assessed. They specifically mention the messages that the ICT division disseminated throughout the organization. On the contrary, they think communication could have been more precise, and that training should contribute to improving the management of cyber-attacks in the future. Table 13 summarizes the main findings referred to the 'Communication' dimension.

5.5 Accountability

It refers to the organization's response to employee violation of information security policies.

The cyber-attack did not seem to have positively increased the sense of accountability. On the contrary, the analysis reveals numerous aspects relating to gaps in this dimension. Two elements stand out: a diluted responsibility of users, who tend to say responsibility falls on System Division technicians and, on the other hand, it seems the organization leaves the control of assumed cyber-risks in the hands of users and their judgment. Table 14 summarizes the main findings referred to the 'Accountability' dimension.

5.6 Governance

It refers to the positioning of information security at the organization (as management's obedience to information security policies or the managerial perception of information security importance).

The attack sustained seems to have reinforced trust in the ICT Division as an organizational guarantor against cyber-attacks. Similarly, it is perceived that this type of threat will be constant and increase, and that in order to face them it is necessary for senior management to prepare the organization by allocating the necessary resources and clarifying roles so as to strengthen the ICT Division. It is also worth mentioning the implicit assumption that high cyber-security standards are incompatible with the research mission of the center. Table 15 includes the main findings associated with this dimension.

Table 12 Interpretative Repertoires of Compliance

Perceived benefits arising from the cyber-attack	Increase of safe behaviors and decrease of 'risky practices' linked to information technologies: - Uninstalling external programs - Observing recommendations against ransomware - Decreased use / download of non-licensed programs
Perceived weaknesses arising from the cyber-attack	Improved regulatory compliance due to memories of the cyber-attack (it could be temporary). Non-compliance is linked to a lack of information on cyber-security norms and protocols. Resolution of the dilemma between production and cyber-security: regulatory non-compliances are justified by saying workers are required to carry out work.

Table 13 Interpretative Repertoires of Communication

Perceived benefits arising from the cyber-attack	Improvement of organizational communication processes. - During the attack: They contributed to address the multiple drawbacks caused - After the attack: They reinforced the security policy and contributed to generating more secure behaviors
Perceived weaknesses arising from the cyber-attack	Need for more specific information on the cyber-attack (organizational improvement opportunity based on lessons learned). Need to reinforce the training and qualification of personnel in the area of cyber-risks.

Table 14 Interpretative Repertoires of Accountability

Perceived benefits arising from the cyber-attack	[No benefits referred to in this dimension]
Perceived weaknesses arising from the cyber-attack	Paradox of responsibility in cyber-security. - Perception that personnel in information systems are responsible for cyber-security. - User with authority to assess and face potential cyber-risks

Table 15 Interpretative Repertoires of Governance

Perceived benefits arising from the cyber-attack	The ICT division as an organizational reference of cyber-security.
Perceived weaknesses arising from the cyber-attack	Need for global planning (by senior management) so as to properly face emergent technology risks. - Greater resource allocation - Improved coordination between ICT and the remaining departments Perception of antagonism between cyber-security and the center's research activities

6 Discussion

The case study presented here has aimed to assess the impact of a cyber-attack on employees' perceptions of cyber-security and to highlight the main interpretative arguments that underpin these perceptions. To do that, a "Perception of ICT security in the work environment" scale was applied in two different moments in time (before and after a cyber-attack), thus favoring a quasi-experimental quantitative design complemented with the application of qualitative research techniques, all within the framework of a mixed methodology research strategy [80]. Three relevant aspects of this study are used for discussion purposes: (a) the impact of a cyber-attack on the perception of ICT security; (b) accountability for cyber-security as a central element of a strong cyber-security culture and; (c) the apparent incompatibility between science (or research activity) and cyber-security.

Firstly, with regard to the impact of the cyber-attack, previous studies [58] revealed that living through a cyber-incident affects employees' perception of cyber-risk relevance and attack response effectiveness. In that sense, this study confirms that experiencing a cyber-attack significantly changes personnel's' perception of ICT security. A greater score after the incident takes shape in a more favorable opinion of the organization's efforts to reinforce preventive behaviors; a greater risk awareness and importance given to information security while carrying out individual work and an increased trust in the information security of the organization interestingly and despite the cyber-attack sustained by the organization are detected too. Somehow, this significant increase in the scale score seems to be partly caused by the considerable communication efforts made by the organization throughout the entire incident. This favorable perception of communicative processes is confirmed by the qualitative analysis of interviews and focus groups. The in-house communication is thought to be 'increasing' and will 'provide results' favoring cyber-security enhancement. The relevant role of organizational communication has already been highlighted in some studies [48].

Having said that, it is worth mentioning that qualitative data shows that despite a perception of improvement in responsible behaviors, there is also an underlying uncertainty that it could be an improvement linked to the fresh memory of the event. In other words, there is a certain doubt on whether non-compliances will increase as time goes by and people forget about the cyber-attack. One of the key findings of this study is that future compliance intentions appear to be more influenced by the negative consequences experienced from the event rather than by adherence to the existing information security policy. However, the case analysis also shows that the experience of a cyber-attack does not automatically guarantee employee secure behavior. In addition, it is important to note how prioritizing the completion of work tasks can potentially undermine cybersecurity practices. Furthermore, the study illustrates the diversity of arguments that influence non-compliance, not only limited to lack of knowledge of protocols or lack of information, but also to behaviors based on alignment with organizational objectives that potentially put cyber-security at risk.

Secondly, with regard to cyber-security accountability, this research shows that responsibility is diluted when it comes to information security. Even if globally it is assumed that ICT is the guardian of cyber-security (formal and documentation responsibility falls within personnel in this department), it is perceived that organizationally there is a wide margin of discretion for users. The shared belief that users have 'too much freedom' or that the organization 'lacks control', points to a potential risk factor relating to cyber-security. In that sense, one should wonder to which extent this wide margin of discretion, without an organizational cyber-risk governance policy restricting this universe of behavioral possibilities, becomes an actual critical risk for cyber-security. In order to minimize or control risks, a culture of cyber-security certainly needs robust cyber-security training programs, as well as the implementation of standards and broadly used protocols fostering safe behaviors amongst all users. Similarly, qualitative analysis results reveal the need for senior managers' commitment as a key step to establishing a strong cyber-security culture, which is a critical element already mentioned by other authors [99]. In essence, an adequate technological governance of cyber-risks inherently entails global planning (considering cyber-threats as a significant challenge for the organization), sufficient economic funds to face those threats and a clear reinforcement of the key role to be played by the ICT Division in the management of cyber-security.

Hence, additional activities reinforcing the newly acquired perception of how cyber-security affects daily work should be adopted by the studied center. These activities should go beyond the usual messages alerting of potential risks but rather focus on putting again the staff under the consequences of a cyber-attack, even if simply simulated.

The research reveals the intricate complexity of organizational determinants in establishing a culture that supports strong information systems security. Several previous studies have identified overconfidence in the organization's technology [57] or individual ignorance and negligence as factors related to most cyber-threats [40]. What is novel in the case study presented here is that an individual sense of technical competence (e.g., to assess potential cyber-risks) could, paradoxically, also become an organizational weakness. In other words, overreliance on technology can be detrimental to security.

Thirdly, this case study provides a specific finding relating to the cyber-security culture of research centers. The qualitative analysis reflects a perception of antagonism between the concepts of cyber-security and research behaviors. This creates a controversial tension between the research purpose of the organization, which requires users to have "ample freedom," and, on the other end of the spectrum, the regulatory aspects of the R&D&I centers, which guide the use of information technologies according to rigorous and restrictive security protocols. According to some employees, "VPN restrictions" or "firewall incompatibilities" are elements justifying non-compliance with cyber-security protocols. That means one should consider the "science - cyber-security" dilemma as an element which needs to be addressed by research centers. The results of this study, therefore, pose crucial questions that demand fundamental reflection on cyber-security within the field of research. For instance, does a robust cyber-security culture clash with a culture that prioritizes innovative research? To what extent can the cyber-security models employed by commercial organizations be adapted to research centers? It is worth noting that, in some cases, the organizational decentralization of R&D&I may entail necessary adjustments or specific developments for the ICT security. In any case, cyber-security is relevant in research centers (such as the one in this case study) because they manage high-value confidential information, which has to be protected from potential cyber-threats. Similarly, the overconfidence of researchers who tend to overestimate their knowledge as users of information and communication technologies (minimizing cyber-risks) could lead to undesired events going beyond the scope of their own work [100]. Resolution of this dilemma should be ensured through a strong awareness of the potential cyber-risks and their consequences at all organizational levels, as well as through clear communication of the benefits of cyber-security as a tool to face those risks. It is also appropriate to reflect on whether or not it is necessary to adapt the security systems to the specificity of the research centers and to their research mission. That would contribute to clarifying this perceived antagonism between science and cyber-security.

This research holds significant practical value for enhancing cyber-security in research centers. Two considerations arise in this regard. Firstly, the commitment of senior management to facilitate an organizational assessment of the cyber incident's impact on employees' perceptions has enabled the collection of accurate information regarding weaknesses (as well as strengths) in addressing cyber-security. Secondly, the study emphasizes the value of employing a mixed methodology, which stands out for its effectiveness and ability to produce insightful findings. The combination of techniques of diverse nature facilitates an in-depth exploration of the intricacies of organizational culture as the foundation of cyber-security. Such an approach can serve as a guide for other similar institutions.

Lastly, this study has some limitations. In terms of quantitative aspects, internal organizational changes hampered comparisons between several units which have changed, in the sense that socio-demographic information in 2022 was not equivalent to that of 2019. For instance, the exclusion of gender as a sociodemographic option in time 2 hinders the ability to compare the impact of cyber-attacks based on gender. Also, the methodological design does allow the development of a causal model between organizational communication and trust in information security. As for qualitative data, this study did not include any focus group involving the participation of senior management, thus losing the opportunity to capture the perceptions and beliefs of managers in this R&D&I center. Furthermore, the existing 'science - cyber-security' dilemma is obtained only for the 2022 assessment of this organization. It would be interesting to compare these results to those of others research centers.

7 Conclusions

Cyber-security is a critical issue for the mission of research organizations that conduct high-quality, cutting-edge research, transfer technology, and promote innovation. The aim of this case study was to assess how a relevant external cyber-attack had affected the perception ICT security among members of a prominent Spanish R&D&I organization. A socio-technical approach was adopted, which conceptualizes cyber-security as a factor resulting from the interaction of technological, behavioral, and organizational factors. The research was developed according to the principles of mixed methods research, with the complementary use of different research techniques (quantitative and qualitative). A survey was conducted before (2019) and three months after the cyber-attack (2022), both to understand how the relevance of ICT security is perceived in the organization. In addition to quantitative information, qualitative techniques (semi-structured interviews, focus groups, and a micro-ethnography) were used after the incident to identify the interpretative repertoires that construct perceptions of cyber-security. The results of the study show, firstly, that the cyber-attack affects perceptions of ICT security, that internal communication seems to play an important role in improving these perceptions, and that some uncertainty remains about the sustainability of the positive behavioral changes observed after the attack. A notable finding from the study is that individual compliance with security policies is a subtle and multifaceted aspect that necessitates continuous awareness programs. The case study underscores how even strong

individual accountability, coupled with a focus on work compliance, can paradoxically exert a negative impact on cyber-security.

A second conclusion is the perceived need for global governance of cyber-security, as opposed to an organizational reality that relies primarily on the goodwill and good work of employees which is perceived as critical in relation to the organizational reality, i.e. it requires thorough planning, sufficient financial resources and a clear reinforcement of the key role of the ICT department in cyber-security management. Importantly, it is recognized that governance should not rest solely on the ICT Division; but also in the strategic apex which plays a primary role in planning, forecasting and resource allocation.

Thirdly, a remarkable element of the study is that it provides insight into the determinants of cyber-security in a large R&D&I center. The case study reflects the existence of an antagonistic view between cyber-security and research behavior, which is erected to justify regulatory violations for research purposes. Balancing scientific research activities with cyber-security protocols and staff compliance emerges as a significant challenge in the management of cyber-culture in R&D&I. This perceived dilemma must be resolved to develop a strong cyber-security culture in research centers without compromising its research mission.

Finally, this study equips research centers with actionable strategies to bolster their cyber-security posture. It highlights the critical role of senior management engagement in assessing the impact of cyber incidents and advocates for the effective use of mixed methods to explore the role of organizational culture in cybersecurity. By offering practical approaches, data collection tools, and insightful findings, the study serves as a valuable resource for similar institutions striving to strengthen their cyber-resilience, preventing attacks and enabling recovery and adaptation.

Appendix 1. Behaviorally anchored rating scale (BARS)

Security of Information and Communication Technologies (ICTs)

It refers to activities implemented by the organization to ensure the integrity of computer systems and the information they contain. It also refers to the risk perception of personnel and the level of compliance with security protocols.

(A) ICT security is paramount to the organization. Personnel are aware of the need to comply with established good practices. Security standards and protocols are perceived as necessary and do not interfere with work execution. ICT systems are constantly adapted to new threats and risks.
(B) The organization makes efforts to ensure ICT security levels are not compromised at any time. Personnel clearly understand that ICT security is a high priority.
(C) The organization takes some measures to maintain ICT security. Personnel are not fully aware of all risks and how to prevent them. Priority is sometimes given to work and other times to security.
(D) Only when a relevant problem occurs, ICT security is put first. Work is prioritized over security. Personnel lack engagement and/or knowledge when it comes to ICT security standards.
(E) ICT security aspects are secondary in the organization. Personnel do not consider security as relevant and issues which may impact security are not taken into account. Security protocols and regulations (where they exist) are perceived as hurdles that can be bypassed.

Author contributions Conceptualization: [Joaquín Navajas; Eulàlia Badia; Rafael Mayo]Methodology: [Joaquín Navajas; Eulalia Badia] Formal analysis and investigation: [Joaquín Navajas; Eulàlia Badia; Laura Jiménez; Maria Jesús Maríjuan], Writing - original draft preparation: [Joaquín Navajas; Eulàlia Badia]; Writing - review and editing: [Joaquín Navajas; Eulàlia Badia; Laura Jiménez; Maria Jesús Maríjuan; Rafael Mayo], Funding acquisition: [Joaquín Navajas; Rafael Mayo]Resources: [Joaquín Navajas; Rafael Mayo]Supervision: [Joaquín Navajas]

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. The present research was conducted with the financial support of Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT).
Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Declarations

Competing interests The authors declare their compliance with the ethical standards established by the Committee on Publication Ethics (COPE) in the planning, execution and presentation of this manuscript. In relation to the data of this study: The data has been obtained on a consensual basis by informing the human participants. - Confidentiality and anonymity of human participants and their data were protected at all times. - The purpose and scope of the study has been reported accurately and honestly. - There was no plagiarism or other forms of research misconduct.

Research data policy and data availability statements The data generated in this research (quantitative and qualitative data) are available from the authors upon reasonable request and with the permission of CIEMAT (Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas).

References

1. Horvath, R.: Research & development and growth: A bayesian model averaging analysis. Econ. Model. **28**, 2669–2673 (2011). https://doi.org/10.1016/j.econmod.2011.08.007
2. Edquist, H., Henrekson, M.: Swedish lessons: How important are ICT and R&D to economic growth? Struct. Chang. Econ. Dyn. **42**, 1–12 (2017). https://doi.org/10.1016/j.strueco.2017.05.004
3. Zhang, M., Wang, L., Jajodia, S., Singhal, A.: Network Attack Surface: Lifting the Concept of Attack Surface to the Network Level for evaluating networks' resilience against zero-day attacks. IEEE Trans. Dependable Secur. Comput. **18** (2021). https://doi.org/10.1109/TDSC.2018.2889086
4. Kelleher, J.D., Tierney, B.: Data Science. The MIT (2018)
5. OECD: OECD Science, Technology and Industry Scoreboard 2017: The digital transformation. Paris (2017)
6. Li, Y., Liu, Q.: A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. Energy Rep. **7**, 8176–8186 (2021). https://doi.org/10.1016/j.egyr.2021.08.126
7. Sen, R.: Challenges to cybersecurity: Current state of affairs. Commun. Assoc. Inf. Syst. **43** (2018). https://doi.org/10.17705/1CAIS.04302
8. Hall, M.: Why people are key to cyber-security. Netw. Secur. 2016. (2016). https://doi.org/10.1016/S1353-4858(16)30057-5
9. Check Point Software: Informe de Seguridad Cibernética 2022 (2022)
10. Craigen, D., Diakun-Thibault, N., Purse, R.: Defining Cybersecurity. Technol. Innov. Manag Rev. **4**, 13–21 (2014). https://doi.org/10.22215/timreview835
11. Liu, X., Ahmad, S.F., Anser, M.K., et al.: Cyber security threats: A never-ending challenge for e-commerce. Front. Psychol. **13** (2022). https://doi.org/10.3389/fpsyg.2022.927398
12. Von Solms, R., Van Niekerk, J.: From information security to cyber security. Comput. Secur. (2013). https://doi.org/10.1016/j.cose.2013.04.004 38:
13. Ogbanufe, O.: Enhancing end-user roles in Information Security: Exploring the setting, Situation, and identity. Comput. Secur. **108** (2021). https://doi.org/10.1016/j.cose.2021.102340
14. Mailloux, L.O., Grimaila, M.R., Colombi, J.M., et al.: System Security Engineering for Information Systems. Emerg. Trends ICT Secur. 5–23 (2014). https://doi.org/10.1016/B978-0-12-411474-6.00001-3
15. da Veiga, A.: Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study. Inf. Comput. Secur. **24**, 139–151 (2016). https://doi.org/10.1108/ICS-12-2015-0048
16. Hemanidhi, A., Chimmanee, S.: Military-based cyber risk assessment framework for supporting cyber warfare in Thailand. J. Inf. Commun. Technol. **16** (2017). https://doi.org/10.32890/jict2017.16.2.8229
17. Spalević, Ž.: Cyber Security as a Global Challenge Today. Cyber Bezb Kao Glob Izazov Današnjice (2014)
18. Chan, S.H., Janjarasjit, S.: Insight into hackers' reaction toward information security breach. Int. J. Inf. Manage. **49**, 388–396 (2019). https://doi.org/10.1016/j.ijinfomgt.2019.07.010
19. Bicakci, S., Gücüyener Evren, A.: Responding cyber-attacks and managing cyber security crises in critical infrastructures: A socio-technical perspective. pp 125–151 (2024)
20. McEvoy, T.R., Kowalski, S.J.: Deriving Cyber Security risks from human and organizational factors – A socio-technical Approach. Complex. Syst. Inf. Model. Q. 47–64 (2019). https://doi.org/10.7250/CSIMQ.2019-18.03
21. Malatji, M., Marnewick, A., von Solms, S.: Validation of a socio-technical management process for optimising cybersecurity practices. Comput. Secur. (2020). https://doi.org/10.1016/j.cose.2020.101846 95:
22. Safa, N.S., Sookhak, M., Von Solms, R., et al.: Information security conscious care behaviour formation in organizations. Comput. Secur. **53** (2015). https://doi.org/10.1016/j.cose.2015.05.012
23. Van Haastrecht, M., Ozkan, B.Y., Brinkhuis, M., Spruit, M.: Respite for smes: A systematic review of socio-technical cybersecurity metrics. Appl. Sci. **11** (2021). https://doi.org/10.3390/app11156909
24. Wiley, A., McCormac, A., Calic, D.: More than the individual: Examining the relationship between culture and information security awareness. Comput. Secur. **88**, 101640 (2020). https://doi.org/10.1016/j.cose.2019.101640
25. ENISA: ENISA Threat Landscape 2022 (2022)
26. Flowerday, S.V., Tuyikeze, T.: Information security policy development and implementation: The what, how and who. Comput. Secur. **61**, 169–183 (2016). https://doi.org/10.1016/j.cose.2016.06.002
27. Staves, A., Anderson, T., Balderstone, H., et al.: A Cyber Incident Response and Recovery Framework to support operators of Industrial Control systems. Int. J. Crit. Infrastruct. Prot. **37** (2022). https://doi.org/10.1016/j.ijcip.2021.100505
28. Shaikh, F.A., Siponen, M.: Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Comput. Secur. **124** (2023). https://doi.org/10.1016/j.cose.2022.102974
29. Wong, L.W., Lee, V.H., Tan, G.W.H., et al.: The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. Int. J. Inf. Manage. **66** (2022). https://doi.org/10.1016/j.ijinfomgt.2022.102520
30. Gillam, A.R., Foster, W.T.: Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. Comput. Hum. Behav. (2020). https://doi.org/10.1016/j.chb.2020.106319 108:
31. Tam, C., Conceição, C., de Oliveira, M. T: What influences employees to follow security policies? Saf. Sci. **147** (2022). https://doi.org/10.1016/j.ssci.2021.105595
32. Bélanger, F., Collignon, S., Enget, K., Negangard, E.: Determinants of early conformance with information security policies. Inf. Manag. **54**, 887–901 (2017). https://doi.org/10.1016/j.im.2017.01.003
33. Chen, X., Wu, D., Chen, L., Teng, J.K.L.: Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. Inf. Manag. **55**, 1049–1060 (2018). https://doi.org/10.1016/j.im.2018.05.011
34. Xu, J., Wang, X., Yan, L.: The moderating effect of abusive supervision on information security policy compliance: Evidence from the hospitality industry. Comput. Secur. **111** (2021). https://doi.org/10.1016/j.cose.2021.102455
35. Ogbanufe, O., Crossler, R.E., Biros, D.: Exploring stewardship: A precursor to voluntary security behaviors. Comput. Secur. **109** (2021). https://doi.org/10.1016/j.cose.2021.102397

36. Li, L., He, W., Xu, L., et al.: Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. Int. J. Inf. Manage. **45** (2019). https://doi.org/10.1016/j.ijinfomgt.2018.10.017
37. Ernst & Young: Is Cybersecurity About More Than Protection? EY Global Information Security Survey 2018–19 (2018)
38. Alharbi, F., Alsulami, M., Al-Solami, A., et al.: The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. Sensors. **21** (2021). https://doi.org/10.3390/s21206901
39. Hasan, S., Ali, M., Kurnia, S., Thurasamy, R.: Evaluating the cyber security readiness of organizations and its influence on performance. J. Inf. Secur. Appl. **58** (2021). https://doi.org/10.1016/j.jisa.2020.102726
40. Quader, F., Janeja, V.P.: Insights into Organizational Security readiness: Lessons learned from Cyber-attack Case studies. J. Cybersecur. Priv. **1**, 638–659 (2021). https://doi.org/10.3390/jcp1040032
41. Zhan, Y., Ahmad, S.F., Irshad, M., et al.: Investigating the role of Cybersecurity's perceived threats in the adoption of health information systems. Heliyon. **10** (2024). https://doi.org/10.1016/j.heliyon.2023.e22947
42. Fernandez De Arroyabe, I., Arranz, C.F.A., Arroyabe, M.F., Fernandez de Arroyabe, J.C.: Cybersecurity capabilities and cyberattacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Comput. Secur. **124** (2023). https://doi.org/10.1016/j.cose.2022.102954
43. Shaikh, F.A., Siponen, M.: Organizational learning from Cybersecurity Performance: Effects on Cybersecurity Investment decisions. Inf. Syst. Front. (2023). https://doi.org/10.1007/s10796-023-10404-7
44. Ngoroge, G.M.: Human Factors Affecting Favourable Cybersecurity Culture-a Case of Small and Medium-sized Enterprises Smes Providing Enterprise Wide Information Systems Solutions in Nairobi City County in Kenya. University of Nairobi (2020)
45. Nissen, V., Marekfia, W.: The development of a data-centred conceptual reference model for Strategic GRC-Management. J. Serv. Sci. Manag. **07**, 63–76 (2014). https://doi.org/10.4236/jssm.2014.72007
46. Stacey, P., Taylor, R., Olowosule, O., Spanaki, K.: Emotional reactions and coping responses of employees to a cyber-attack: A case study. Int. J. Inf. Manage. **58** (2021). https://doi.org/10.1016/j.ijinfomgt.2020.102298
47. Li, L., Xu, L., He, W.: The effects of antecedents and mediating factors on cybersecurity protection behavior. Comput. Hum. Behav. Rep. (2022). https://doi.org/10.1016/j.chbr.2021.100165 5:
48. Corradini, I., Nardelli, E.: Building Organizational Risk Culture in Cyber Security: The Role of Human Factors. In: Advances in Intelligent Systems and Computing (2019)
49. Alshaikh, M.: Developing cybersecurity culture to influence employee behavior: A practice perspective. Comput. Secur. (2020). https://doi.org/10.1016/j.cose.2020.102003 98:
50. Jampen, D., Gür, G., Sutter, T., Tellenbach, B.: Don't click: Towards an effective anti-phishing training. A comparative literature review. Human-centric Comput. Inf. Sci. 10 (2020)
51. Butavicius, M., Parsons, K., Pattinson, M., McCormac, A.: Breaching the human firewall: Social engineering in phishing and spear-phishing emails. In: ACIS 2015 Proceedings – 26th Australasian Conference on Information Systems (2015)
52. Willing, M., Dresen, C., Gerlitz, E., et al.: Behavioral responses to a cyber attack in a hospital environment. Sci. Rep. **11** (2021). https://doi.org/10.1038/s41598-021-98576-7
53. Hepfer, M., Powell, T.C.: Make cybersecurity a strategic asset. MIT Sloan Manag Rev. **62**: (2020)
54. Ho, S.M., Gross, M.: Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness. Comput. Secur. (2021). https://doi.org/10.1016/j.cose.2021.102357 108:
55. Ben-Asher, N., Gonzalez, C.: Effects of cyber security knowledge on attack detection. Comput. Hum. Behav. **48**, 51–61 (2015). https://doi.org/10.1016/J.CHB.2015.01.039
56. IBM Security: The cost of a data Breach Report. Produced jointly between ponemon institute and IBM security (2020)
57. Butavicius, M., Parsons, K., Lillie, M., et al.: When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. Comput. Secur. **98** (2020). https://doi.org/10.1016/j.cose.2020.102020
58. Gehem, M., Usanov, A., Frinking, E., Rademaker, M.: Assessing cyber security. A meta-analysis of threat, trends, and response to cyber attacks (2015)
59. Kanampiu, M., Anwar, M.: Privacy Preferences vs. Privacy Settings: An Exploratory Facebook Study. In: Advances in Intelligent Systems and Computing (2019)
60. Conzola, V.C., Wogalter, M.S.: A communication–human information Processing (C–HIP) approach to warning effectiveness in the workplace. J. Risk Res. **4**, 309–322 (2001). https://doi.org/10.1080/13669870110062712
61. Fischer-Hübner, S., Alcaraz, C., Ferreira, A., et al.: Stakeholder perspectives and requirements on cybersecurity in Europe. J. Inf. Secur. Appl. **61**, 102916 (2021). https://doi.org/10.1016/j.jisa.2021.102916
62. Dang-Pham, D., Pittayachawan, S., Bruno, V.: Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. Comput. Hum. Behav. **67**, 196–206 (2017). https://doi.org/10.1016/j.chb.2016.10.025
63. Patterson, C.M., Nurse, J.R.C., Franqueira, V.N.L.: I don't think we're there yet: The practices and challenges of organisational learning from cyber security incidents. Comput. Secur. **139** (2024). https://doi.org/10.1016/j.cose.2023.103699
64. da Veiga, A., Martins, N.: Improving the information security culture through monitoring and implementation actions illustrated through a case study. Comput. Secur. **49**, 162–176 (2015). https://doi.org/10.1016/j.cose.2014.12.006
65. Microsoft: Microsoft Digital Defense Report 2022 (2022)
66. Smith, S.: Five Cybersecurity Insights for the Public Sector. In: (2019). https://www.tenable.com/blog/five-cybersecurity-insights-for-the-public-sector
67. Toapanta, S.M.T., Cobeña, J.D.L., Gallegos, L.E.M.: Analysis of cyberattacks in public organizations in Latin America. Adv. Sci. Technol. Eng. Syst. **5**, 116–125 (2020). https://doi.org/10.25046/aj050215
68. Riggs, H., Tufail, S., Parvez, I., et al.: Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. Sensors 23 (2023)
69. Hijji, M., Alam, G.: A Multivocal Literature Review on growing Social Engineering based Cyber-Attacks/Threats during the COVID-19 pandemic: Challenges and prospective solutions. IEEE Access. **9**, 7152–7169 (2021). https://doi.org/10.1109/ACCESS.2020.3048839
70. Aman, W., Al Shukali, J.: A classification of essential factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations. Int. J. Adv. Comput. Sci. Appl. **12**: (2021)
71. World Economic Forum: Principles for Board Governance of Cyber Risk (2021)
72. da Veiga, A., Astakhova, L.V., Botha, A., Herselman, M.: Defining organisational information security culture—perspectives from academia and industry. Comput. Secur. **92**, 101713 (2020). https://doi.org/10.1016/J.COSE.2020.101713

73. Ocloo, C.M., da Veiga, A., Kroeze, J.: A Conceptual Information Security Culture Framework for Higher Learning Institutions. In: IFIP Advances in Information and Communication Technology (2021)
74. Moore, G., Khurshid, Z., McDonnell, T., et al.: A resilient workforce: Patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. BMC Health Serv. Res. (2023). https://doi.org/10.1186/s12913-023-10076-8 23:
75. INDRA: SIA despliega la nueva red de comunicaciones ultrarrápidas y seguras de RedIris para universidades y centros científicos por 13 millones de euros. In: (2021). https://www.indracompany.com/es/noticia/despliega-red-comunicaciones-ultrarrapidas-seguras-rediris-universidades-centros-cientificos)
76. EECTI: Estrategia Española de Ciencia, Tecnología e Innovación 2021–2027. Minist Cienc e Innovación (2021)
77. Tang, M., Li, M., Zhang, T.: The impacts of organizational culture on information security culture: A case study. Inf. Technol. Manag. **17**, 179–186 (2016). https://doi.org/10.1007/S10799-015-0252-2
78. Zoppelt, M., Tavakoli Kolagari, R.: What today's serious cyber attacks on cars tell us: Consequences for automotive security and dependability. In: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 270–285. Springer (2019)
79. Johnson, R.B., Onwuegbuzie, A.J.: Mixed methods research: A Research Paradigm whose time has come. Educ. Res. **33**, 14–26 (2004). https://doi.org/10.3102/0013189X033007014
80. Edgar, T., Manz, D.: Research Methods for Cyber Security. Syngress (2017)
81. Creswell, J.W., Hanson, W.E., Clark Plano, V.L., Morales, A.: Qualitative research designs. Couns. Psychol. **35**, 236–264 (2007). https://doi.org/10.1177/0011000006287390
82. Greene, J.C., Caracelli, V.J., Graham, W.F.: Toward a conceptual Framework for mixed-method evaluation designs. Educ. Eval Policy Anal. **11**, 255–274 (1989). https://doi.org/10.3102/01623737011003255
83. Real Decreto 311/2022, de 3 de Mayo, Por El que se regula El Esquema Nacional de Seguridad. (2022)
84. Klieger, D.M., Kell, H.J., Rikoon, S., et al.: Development of the behaviorally anchored rating scales for the skills demonstration and Progression Guide. ETS Res. Rep. Ser. **2018**, 1–36 (2018). https://doi.org/10.1002/ets2.12210
85. Badia, E., Navajas, J., Losilla, J.M.: Safety culture in the Spanish nuclear power plants through the prism of high reliability organization, resilience and conflicting objectives theories. Appl. Sci. **11**, 1–25 (2021). https://doi.org/10.3390/app11010345
86. Alvehus, J., Crevani, L.: Micro-ethnography: Towards an Approach for attending to the multimodality of Leadership. J. Chang. Manag. **22**, 231–251 (2022). https://doi.org/10.1080/14697017.2022.2081245
87. IBM Corp: IBM SPSS Statistics for Windows, Version 28.0 (2021)
88. Anderson, J.C.: An Approach for Confirmatory Measurement and Structural Equation Modeling of Organizational Properties. Manage. Sci. **33**, 525–541 (1987). https://doi.org/10.1287/mnsc.33.4.525
89. Stevens, J.: Applied Multivariate Statistics for the Social Sciences, 4th edn. Lawrence Erlbaum Associates, Mahwah, N.J. SE - (2002)
90. Merenda, P.F.: A Guide to the Proper Use of Factor Analysis in the Conduct and Reporting of Research: Pitfalls to Avoid. (2019). https://doi.org/10.1080/07481756.1997.12068936 30:156–164.
91. Cronbach, L.J.: Coefficient alpha and the internal structure of tests. Psychometrika. **16**, 297–334 (1951). https://doi.org/10.1007/bf02310555
92. Nunnally, J.C., Bernstein, I.H.: Psychometric Theory. McGraw-Hill, New York, USA (1994)
93. Domínguez, L., Sergio, A., Soto, C.: Intervalos de confianza del coeficiente alfa de Cronbach. 1–4 (2015)
94. Taylor, S., Bogdan, R.: Introducción a Los métodos Cualitativos, 3rd edn. Ediciones Paidos (2000)
95. Glaser & Strauss: The Discovery of Grounded Theory. Aldine Publishing Company, Chicago (1967)
96. Potter, J., Wetherell, M.: Discourse and Social Psychology: Beyond Attitudes and Behaviour. - Open Research Online (1987)
97. Fujs, D., Mihelič, A., Vrhovec, S.L.R.: The power of interpretation: Qualitative methods in cybersecurity research. In: ACM International Conference Proceeding Series. Association for Computing Machinery (2019)
98. Pimentel, J.L.: Some biases in Likert scaling usage and its correction. Int. J. Sci. Basic. Appl. Res. **45**, 183–191 (2019)
99. Yeoh, W., Wang, S., Popovič, A., Chowdhury, N.H.: A systematic synthesis of critical success factors for cybersecurity. Comput. Secur. **118**, 102724 (2022). https://doi.org/10.1016/j.cose.2022.102724
100. Sütterlin, S., Lugo, R.G., Ask, T.F., et al.: Augmented Cognition. The Role of IT Background for Metacognitive Accuracy, Confidence and Overestimation of Deep Fake Recognition Skills. Springer International Publishing, Cham (2022)