SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIES NO. 187

DIGITAL TRUST AND AWARENESS SECURITY OF THE NETWORK IN THE NEW ECOSYSTEM OF VALUE EXCHANGE (CONSUMER-ENTERPRISE)

Wiesława CAPUTA[1*], Izabela KRAWCZYK-SOKOŁOWSKA[2], Mariola GRZEBYK[3], Małgorzata STEC[4]

[1] Uniwersytet WSB Merito w Poznaniu; wieslawa.caputa@chorzow.merito.pl, ORCID: 0000-0002-0955-9308
[2] Faculty of Managment, Czestochowa University of Technology; i.krawczyk-sokolowska@pcz.pl, ORCID: 0000-0002-2784-1577
[3] Institute of Economics and Finance, University of Rzeszów; mgrzebyk@ur.edu.pl, ORCID: 0000-0003-1107-0250
[4] Institute of Economics and Finance, University of Rzeszów; mstec@ur.edu.pl, ORCID: 0000-0003-0185-4510
* Correspondence author

Purpose: The key aim of the article is to demonstrate that creating awareness of the network's potential is related to the need to develop and implement a digital trust model also on the client's side.
Methodology: The implementation of the goal is based on: a critical analysis of literature and the analysis of statistical data and reports containing the results of representative research focused on the attitudes and behaviors of enterprises and consumers in the context of their digital awareness. The research was carried out using a systemic approach and reference was made to behavioral concepts of personality.
Findings: We show that:
- a low level of awareness does not preclude digital trust in the provider, but the resistance to trust increases with increasing awareness of network security and translates positively into the dually defined value for the client,
- the need to build a model of trust from the customer's perspective.
Resarch limitation: Our work has limitations. Analyzing the client's awareness only through behavior, referring to a limited extent to social and specific factors determining human personality. We omit the issue of identifying the factors determining trust in the context of the duration of the relationship.
Practical implications: Basing the awareness of the network potential on the triad of perception, action, knowledge can point the way to establishing network awareness and digital trust in the enterprise. It can be a guideline to search for factors determining their formation and measures of effectiveness of activities undertaken in this area.
Social implications: The entire process of building a safety culture - not only of the enterprise, but also of the entire society - can be based on the (PAK) approach. The identified factor may be important for educational activities.
Originality/value The dominant part of research focuses on the search for and implementation of trust models from the perspective of bidders. However, there is a lack of research that considers digital trust from the customer's perspective and connects it with the awareness of

network security. The article is addressed to scientists and practitioners who are interested in creating digital awareness and digital trust in online relationships.

Keywords: awareness of network potential, digital trust, customer value, ecosystem.

Category of the paper: conceptual paper.

1. Introduction

One of the most significant changes in the environment is the ongoing digitization process. It is commonly emphasized that the digital progress observed in recent years has translated into the creation of a wide range of systems with enormous possibilities (Wirtz et al., 2018).

With the dynamic development of the above-mentioned solutions, more and more often there is talk not only about the need to implement them or multidimensional use, but also about the need to ensure the safety of their use.

Practice confirms the growing number and cost of cyberattacks, despite the systematic implementation of new security solutions. Cybercrime research entities around the world indicate that the expanding threat landscape and new business innovations translate into an increase in the number of cyberattacks (Ninth Annual Costof Cybercrime Study, 2019). This also applies to the Polish economy, where the number of cyberattacks increased by 46% in 2022 alone.

According to PwC data, registered acts of cyber-aggression in 33 percent cases translated into financial losses, in 31 percent resulted in the disclosure or modification of data. In 16 percent contributed to the loss of the company's reputation. TNS reports that one in three large domestic companies expect a major attack in the next three months (Lobschat et al., 2021).

The process of digital transformation now applies to everything and everyone, and thus creates a new ecosystem of value exchange. This ecosystem creates new opportunities for exchange participants, but also poses new challenges and creates new threats.

From the business perspective, changing the ecosystem of establishing and developing relationships with customers is of key importance. These relations determine the capital supply to the enterprise, and thus its value. This relationship is based on a dually defined but mutually correlated customer value (Caputa et al., 2021). Research shows that the customer value defined from the perspective of both sides of the relationship is related to customer satisfaction, closeness, trust and commitment (Payne et al., 2008; Caputa, 2020; Rouhi, Geiger, 2023). Let us consider these factors as universal value-creating factors. However, we see the need for a broader and more comprehensive embedding of these factors in the new virtual exchange ecosystem, which is not immune to multidimensional threats.

The openness of this ecosystem, its network character and its software-based basis make it necessary to base it on relationships between not only the company and the client, but also network users, regardless of their intentions in using the software to make contact.

Such embedding, on the one hand, allowed us to show that in the new ecosystem of exchange, the potential of network awareness and the ability to use it is not only a factor determining the dually defined customer value, but also a factor that necessitates a new look at trust.

We pose the question whether, in a world dominated by new technologies that can be used for various purposes, it is in the interest of the client to trust the offer, or rather to be resistant to trust.

We assume that this resistance increases with the increase in network security awareness and translates positively into dually defined value for the client.

The key aim of the article is to demonstrate that creating awareness of the network's potential is related to the need to develop and implement a digital trust model also on the client's side.

We base the implementation of the indicated goals on literature studies and qualitative research based on a review of statistical data and reports containing the results of the represented research focused on the basics and behavior of customers in the digital environment. Indicating the relationships between: customer value, awareness of network security, digital trust and trust resistance, we rely on the purchasing process implemented in the e-commerce industry. It is the fastest growing industry that engages consumers in a multidimensional way, allowing them to present the entire purchasing process.

Striving to achieve the goals indicated in the following points:

1. We present a model of customer value creation and identify universal factors determining this value in a new ecosystem of customer-enterprise value exchange.
2. We define the potential of network awareness in the context of the security of both sides of the relationship.
3. Present the current concepts of defining trust, demonstrating the necessity of separating digital trust and its analysis in relation to the awareness of online security.
4. Based on empirical research, we identify the declared and actual customer awareness by relating the research results to the image of the company-customer relationship on the E-commerce market in Poland. On this basis, we indicate the relationship between trust and awareness of the network's potential.

As a result of the conducted research, we demonstrate the legitimacy of creating customer resilience.

Any use of technology that is not intended by both parties to the relationship temporarily or gradually affects the mutual relationship, changing the perceived benefits, threats and threats of the relationship. Therefore, we demonstrate the need to seek and implement trust models not only on the part of the offerer, but also the client.

2. The model of customer value creation in the new ecosystem of customer-enterprise value exchange

Starting from the last decade of the 20th century, we have been observing a progressing digitization process, which is directly related to the increase in the use of digital and computer technologies

Consequently, all processes of individual and collective activity are shaped by the new technological medium. The increase in the turbulence of the environment is accompanied by an increase in the number of interactions that, while setting the direction of development, are also unpredictable, which translates into an increase in risk, which increasingly concerns the security of the multidimensional use of technology and the potential of network users.

In the light of the above considerations, it is reasonable to say that the ongoing digitization process has created conditions for establishing relationships and interactions with many entities in real time to achieve multidimensional goals in open space. These conditions are conducive to the development of ecosystems. It should be emphasized, however, that this category is not uniformly defined.

Table 1.
Overview of selected concepts for defining the ecosystem

Ecosystem	Source	Source Definition
Business ecosystem	Moore, J.F., 1993. Predators and prey. A new ecology of competition. *Harvard Business Review, 71(3),* 75-86.	Is the company's external environment.
	Eisenhardt, K.M., Galunic, D.C., 2000. Coevolving: at last, a way to make synergies. *Harvard Business Review , 78*, 91-101.	Has its roots in the idea of a value network and can be seen as a group of companies that simultaneously create value by combining their skills and assets.
A sustainable entrepreneurial ecosystem	Cohen, B., 2006. Sustainable valley entrepreneurial ecosystems. *Business Strategy and Environment, 15,* 1-14.	Interconnected groups of actors in a local geographic community committed to sustainable development by supporting and facilitating new sustainable ventures.
Entrepreneurial ecosystem	Mason, C., Brown, R., 2014. Entrepreneurial ecosystems and growth oriented entrepreneurship. *Final Report to OECD, 30, 1.* Paris, 77-102.	A collection of interconnected entrepreneurial entities, entrepreneurial organizations, institutions and entrepreneurial processes that formally and informally come together to connect, mediate and manage results in a local entrepreneurial environment.

Cont. table 1.

Ecosystem entrepreneurship	Malecki, E.J., 2018. Entrepreneurship and entrepreneurial ecosystems. *Geography Compass, 12, 3, e12359*.	Dynamic local social, institutional and cultural processes and actors that encourage and enhance the creation and growth of new businesses.
	Spigel, B. 2017. The relational organization of entrepreneurial ecosystems. *Entrepreneurship Theory and Practice, 41(1),* 49-72.	Combinations of social, political and cultural elements in the region that support the development and growth of innovative start-ups and encourage start-up entrepreneurs and other entities to take risks related to establishing, financing and otherwise supporting high-risk ventures.
	Cantner, U., Cunningham, J.A., Lehmann, E.E., Menter, M., 2021. Entrepreneurial ecosystems: a dynamic lifecycle model. *Small Business Economics, 57, 1,* 407-423.	Interactions between nearby entities disseminating and commercializing new ideas through intrapreneurship. The basic function of ecosystem activity is entrepreneurship, representing the diffusion of previously uncommercialized knowledge and ideas.
Innovation ecosystem	Adner, R., 2006. Match your innovation strategy to your innovation ecosystem. *Harvard Business Review, 84(4),* 98-107; Frenkel, A., Maital, S., 2014. Mapping national innovation ecosystems: Foundations for policy consensus. In: Mapping national innovation ecosystems: Foundations for policy consensus (edward elg).	Interactions between different industry and innovation actors or stakeholders. The most important of these actors are enterprises - large and small companies, start-ups and entrepreneurs, financial markets, universities and research-related organizations and NGOs and government institutions.
	Shaw, D.R., Allen, T., 2018. Studying innovation ecosystems using ecology theory. *Technological Forecasting and Social Change , Vol. 136, November,* 88-10.	Interconnections of business models with paths that transfer material and information resources, as well as values. Business models are similar to an organism's genome in that they describe the limits of feeling, acting, and understanding.

Source: own elaboration.

Taking into account the overview of definitions of selected concepts of defining ecosystems presented in Table 1, it is not difficult to prove that each ecosystem has its actors Each type of ecosystem is directly geared towards value co-creation (Aarikka-Stenroos, Ritala, 2017; Kapoor, Lee, 2013). However, co-creation is driven by different processes in different types of ecosystems, Unlike networks, co-creation of value in ecosystems does not necessarily involve explicit principles of value capture (Bouncken et al., 2020). Importantly, a multi-stakeholder approach is taken in co-creation of value in ecosystems (Bacon, Williams, 2021), going beyond the classical linear, i.e. sequential approach to joint value creation. Indeed, in ecosystems, co-creation of value with customers and even communities with customers (Prahalad, Ramaswamy, 2004) goes much further, involving co-creation with other external actors and even entire networks of actors (Vargo, Lusch, 2011). This confirms the earlier statement that, regardless of the type of ecosystem, each has a purpose.

It is generally accepted that the main goal of a company is to create value. This process takes place in changing environmental conditions. The result of this process from the company's perspective should be the multiplication of the invested capital (Jonek-Kowalska, 2012). It is therefore in the interest of the company to acquire such a client who is profitable and able

to provide the capital desired by the company for the longest possible period (Alsyouf, 2007). The consequence of this is the need to establish and develop lasting and profitable relationships with customers, which are based on dually defined customer value (Caputa et al., 2021).

From the customer's perspective, this value reflects the ability of the product offered on the market to solve its subjective, multidimensional needs (Swenney, Soutar, 2001, Caputa, 2020).

The customer value assessed from the company's perspective is not only directly related to the assessment of the customer's readiness and ability to make purchases (transaction value), but also his readiness and ability to launch such an information message that can contribute to the value creation process (resource value) (Payne et al., 2008; Rouhi, Geiger, 2023).

There are correlations between the value for the customer and the value of the customer. As a result, the dually perceived customer value can be defined as a complex bundle of benefits: economic, technical, emotional and social contained in the product and accompanying services, which arises as a result of the involvement of the company's knowledge resources and related value network partners, creating the opportunity to obtain capital supply securing the implementation of the company's interests.

Maximizing the above-mentioned benefits in the long term for both sides of the relationship raises the need to transform contacts into lasting and profitable relationships.

Achieving such an effect requires not only creating a state of satisfaction, but also maintaining and developing ties, which, along with their duration, should be increasingly based on trust and commitment of the parties (cognitive-emotional phase).

This increases the likelihood of a transition from the customer's intention (cognitive loyalty) to the willingness to take action (actional loyalty). Creating such relationships requires interactions that boil down to a constant game between the subjective expectations of both parties to the relationship and the objective possibilities of satisfying them (Caputa et al., 2021).

However, the classic value creation process indicated in the figure cannot be separated from the ongoing digitization process, which, by transferring business processes to the network, creates:

- a new relationship that is established through technology with known, unknown and invisible entities operating in the network,
- a new customer who no longer wants to be a passive participant in the exchange,
- a new environment, created with the use of information technology, which in a multimedia way creates a computer vision of objects, space and events, enables interaction and the flow and processing of information in real time.

As a result, digitization changes the purchase and sale process, opens the way to obtaining information and knowledge from many sources. Each network user may: support other users in making decisions and use their support, share experiences, create a virtual community of brands, or have a negative impact on brand perception, create communities and/or participate in virtual communities and use them for their own purposes, warn against threats, including

those related to computer use, network activity or the use of software, and to be the creator of such threats.

Therefore, we are dealing with the opening of the process of creating customer value, which, based on the network of relationships and interactions, can be used by both parties to the relationship to achieve individual and/or common goals, with the support of other entities and institutions. Therefore, we can talk about a new ecosystem of value exchange, which is evolving along with the ongoing digitization proces (Figure 1).

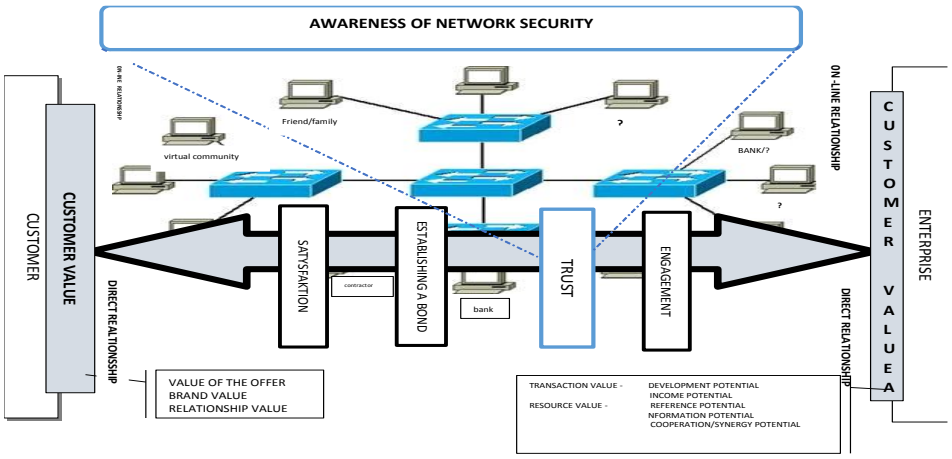

Figure1. Model of creating relations with clients.

Source: own study.

This ecosystem offers a range of opportunities, but it is based on the use of technology and networks. As a result, both sides of the relationship must be willing and able to use it to meet their own needs. As a consequence, this means that each element of the dually defined customer value and each factor determining the durability and profitability of the relationship determines the awareness of the network's potential and the ability to use it.

3. Awareness of the network's potential and the ability to use it

The category of consciousness has no uniform interpretation (Vimal, 2009). Consciousness is the state or ability to perceive, feel, or be aware of events, objects, or sensory patterns (Najafi, 2012). In the general sense, consciousness is identified with the intellectual state of individuals or society, which results from the degree of knowledge, understanding and rational evaluation of facts or events (Pazio, Formanowska, 2002). It is also associated with knowledge and the ability to use it rationally in the context of an emerging problem (Szumlicz, 2006). In the narrow sense, consciousness is a measure or indicator of the intellectual level of individuals and social groups.

Therefore, the concept of consciousness is associated with the ability to generate, process and use information. This ability is largely conditioned by human personality, i.e. "a set of permanent and variable psychophysical features that are associated with all human activities, experiences and needs at the physiological, characterological, intellectual and spiritual level" (Horzyk, 2012).

We assume that although consciousness remains associated with knowledge, i.e. with the intellectual level, it is in fact a mental state (a set of mental states) in which the individual is aware of his own thought processes (self-awareness) and phenomena occurring in the external environment and is able to react to them According to P. Carruthers, the degree to which a person "is aware of an object/event is actually the degree of intensity and accuracy of the perceptions generated by that object/event, resulting from the degree of attention paid" (Carruthers, 2003). This perception of consciousness is related to the need for security.

Building a customer-enterprise relationship in the virtual space is inextricably linked to the need to meet the need for security. In general terms, security means a state in which an individual feels confident and does not identify any threats. It is a subjective state (Williams, 2008). Therefore, it can be assumed that security is a function of the two main risk factors and the probability of its occurrence.

This need, in a new environment, takes on a new dimension. The threat, as a rule, is not material. Its source is the space where data and information processing and interactions in ICT networks take place (Zhang, 2020). The source of the threat can be found at every stage of building a relationship, even before establishing a transactional contact (Caputa, 2020). These threats can have a negative impact on customer satisfaction, trust and engagement. Therefore, the risks must be important to both the customer and the seller.

Therefore, security awareness should be associated on the one hand with the customer's willingness and ability to perceive these threats, and on the other hand with the tendency to take action against their negative effects, which is related to the risk assessment of the threat and confidence in protective measures. In a virtual network, digital situational awareness is required (Tadda et al., 2006), which is a three-step process that includes recognition (or awareness of the current network situation); understanding (or awareness of malicious behavior in the current network situation); and projection (evaluation of malicious behavior in the current network situation). Awareness of the potential of the digital network means the ability of the general public to use online services and information and communication technologies effectively. Using a digital system requires clients to be computer literate, understand digital documents, and websites, and the risks involved (Tripathi, Gupta, 2020) Awareness of digital relationships plays an important role in ensuring effective digital communication as participants need to be aware of behaviors and responsibilities people with whom they interact. Awareness of potential includes the ability and knowledge necessary to use digital tools and the ability to sense, know and perceive digital developments around the individual (Karakuş, Kılıç, 2022). In an open space, technology can be used by others in a way that puts the well-being of the client or the

reputation of the company at risk (Caputa, 2020). As a result, the course of the relationship and its effects also depend on the awareness of network threats and the ability to limit them.

Threats resulting from the need to use technology and the use of network relationships require a new look at trust as a factor determining customer value. If an unknown network user, through the use of technology and the network, can interfere in the course of the relationship in a way that reduces the benefits of both parties to the relationship. Each party to the relationship must, on the one hand, build relationships based on trust, but on the other hand, demonstrate resistance to digital trust.

4. Digital trust and determinants of trust

Trust is an interdisciplinary concept. In the literature, this concept is to: a kind of belief in the good will of the other subject (Seligman, 1997), created in conditions of non-transparency of his intentions and will, *a bet made on the uncertain future actions of other people* (Sztompka, 2005) the belief that the results of the actions of others will be appropriate from the perspective of the evaluator the expectation of a person or group that they can rely on the word or promise of another person or group (Rotter, 1980) the expectation of favorable behavior from someone in a socially precarious situation based on the knowledge of his inclinations (Yamagishi, 2002).

Trust means the subjective belief of the parties to the relationship regarding maintaining credibility in the context of potential risk. Due to the subjective nature of trust, it may result from relational and individual characteristics. The attributes of relational trust occur and relate to relationships with other entities, and the dimensions of the individual are derived from the individual's own characteristics.

Among the factors affecting trust, conditions should be distinguished that include internal and/or external properties, such as the mental state of the individual and the social/political relationships of the entities (Cho et al., 2015). Risk critically affects the relationship of trust, i.e. readiness to taking risks under conditions of uncertainty (Luhmann, 1979). Faith, i.e. belief based on irrational grounds (Castelfranchi, Falcone, 2010). Fear, or "perceived risk" that is unbearable or unmanageable as extreme distrust. A feeling is something that the subject "feels" in the context of the subject, a feeling formed on the basis of experiences, dispositions, intuitions, knowledge and/or implicit learning (Castelfranchi, 2009). Dunn and Schweitzer show that positive emotional well-being (e.g. happiness, hope) increases trust, while negative emotional well-being (e.g. fear, guilt) lowers trust (Dunn, Schweitzer, 2005). Belief, fear, feeling and emotional well-being are components related to individual characteristics that affect trust. On the other hand, the group of conditions affecting trust includes controls (Castelfranchi, Falcone, 2010), which can complement trust and lead to its growth or loss. In the context of trust and risk, there is also institutional trust associated with norms and regulations to protect

the parties to a relationship of threat or abuse of trust. An important element of trust is cooperation recognized as a result of the relationship, in which the foundation is the durability of the relationship based on the possibility of mutual reward and reciprocity of benefits, i.e. cooperation of behavior for others (Gambetta, 1988). Another factor is the transfer of responsibility through the process of delegating activities to other entities (Castelfranchi, 2009).

Digital trust "underlies every digital interaction" (Gartner, 2017). Trust in digital services creates a new type of relationship and addresses certain trust in people and technological processes to create a secure digital world (Joyce, 2018). Digital trust reflects the customer's belief that the organization collects, stores and uses their information responsibly and that they protect that information. (Accenture, Digital Trust…, 2017) This trust is seen as a separate but potentially co-existing mechanism to reduce the uncertainty and complexity of transactions and relationships in electronic markets. The basis for such action is the ability to communicate in an open space, which can be reduced to the ability to share oneself. According to M. Heidegger, the dynamically advancing digitization process allowed to overcome the distance, but did not create closeness (Fors, 2010). The customer can therefore trust companies, buy their products and recommend them to others, which, however, does not mean that they will be immune to the actions of competing entities. It also does not mean that he has a sense of personal security and the processes in which he participates. The company must therefore strengthen its credibility and the level of acceptability, which is facilitated by the inclusion of the customer in the value creation process, which is related to his involvement.

As a result, the customer's trust can be combined with a subjective assessment of the company's willingness and ability to solve its problem, made under conditions of risk and uncertainty. The risk decreases with the increase in the level of knowledge, which means that the customer experience and the intensity and quality of knowledge transfer between the indicated parties to the relationship positively translate into the level of trust.

This statement is confirmed by research which shows that one of the important correlates of trust are previous experience and the prospect of repeated transactions with the bidder (Williamson, 2014). The quoted studies also indicate other determinants, such as: trust or distrust as an individual feature of the client's personality, factors related to the level of service and competence of people directly serving the client, or the level of legal and institutional protection of the client.

A significant impact on trust is also exerted by current impressions (Delgado-Ballester, Manuera-Aleman, 2000), which in the "flat world" should also be combined with the possibility and consequences of establishing relationships by the client and the company in the network.

Consequently, this means that trust, remaining in the network of: suppliers, distributors, subcontractors, producers of related products and other entities that affect the creation and delivery of the company's products and are the subject of their impact, is a derivative of the ecosystem in which the exchange takes place. Therefore, when creating relationships based on trust, the company faces the need to influence the entities of the ecosystem in such a way that

it is conducive to building positive customer experiences and impressions, and such an impact on the customer that strengthens the bond between him and the company.

5. Research methodology

Literature studies have shown that the progressive development of digital transformation transfers relationships to the network, which enables interactions between all its users. This is conducive to the development of ecosystems, which by nature are oriented towards co-creation of value (Aarikka-Stenroos, Ritala, 2017), with the involvement of many actors (Bacon, Williams, 2021).

This blurs the boundaries of the enterprise and expands the client's space. Based on the systemic approach (Jackson, 2000) and referring to the achievements of institutional economics and relationship marketing, we assume that the company and the client are entangled in a network of relationships and interactions. This network is now being created through technology. As a result, the establishment of a relationship and its development with the participation of its users at the very beginning depends on the acceptance of the use of technology and the ability to use it in a multidimensional way to build a relationship based on dually defined customer value. Thus, the awareness of the network's potential, i.e. the readiness and ability of both parties to the relationship to use technology, create and use the network's potential, determines the value of the customer. This awareness cannot be separated from the threats resulting from the use of technology as well as relationships and interactions established on the web.

Awareness of online security in the context of creating customer value becomes the main subject of our research. We base this study on the triad: perception, action, knowledge (PAK).

Consciousness, being a set of mental states, is therefore related to personality. Referring to the behavioral concepts of personality (Pawlov, Watson, Skinner, Hull) we assume that a person throughout his entire personal and social development, as a result of the influence of positive stimuli or negative, learns various forms of behavior and reactions, also under the influence of rewards and punishments. As a result, his awareness changes through gaining experience or obtaining information. This leads to the following assumptions:

- the leading factor determining network security awareness is age (H1),
- there is a difference between the declared and real potential of network security awareness (H2).

The acceptance of technology in establishing and developing relationships is closely related to trust. In the digital world, this trust applies to the technology itself as well as to the entity that uses it. As a consequence, the trust that underpins any lasting relationship is becoming digital. Just like awareness, trust is related to a person's personality. The key objective of the study is therefore to identify the relationships between the awareness of the network's potential, digital trust and customer value.

We pose the question whether, in a world dominated by new technologies that can be used for various purposes, it is in the customer's interest to trust the offer and the way to satisfy the need, or rather to be resistant to trust.

We assume that a low level of awareness does not preclude digital trust in the provider, but the resistance to trust increases with increasing awareness of network security and translates positively into the dually defined value for the client (H3).

This is a new context of research, which, unlike the previous ones, does not focus on the company, but on the client as an entity who, being entangled in the network of relationships established through technology, has to take care of his own safety, and thus create his own trust model.

Striving to achieve the indicated goals and hypotheses, apart from literature studies, we rely on the analysis of statistical data and the results of representative research relating to the attitudes and behavior of consumers in the digital world, with particular emphasis on the Polish e-consumer.

6. Study results

6.1. Awareness of the network's potential and trust in the light of research – the perspective of cybersecurity

The legitimacy of the construction of the triad based on three links: perception, action and knowledge is confirmed by the research on cybersecurity awareness that was carried out in 2019 on a sample of 1005 Americans (Consumers' Awareness, 2019). This research focused on answering the question whether consumers are aware of the threats related to privacy and information security on the Internet and how they behave when it comes to protection against cyber threats. The distribution of answers to the question *how do they feel about cybersecurity* Indicated in Figure 2 clearly shows that the majority of respondents declare the existence of a knowledge gap in the field of cybersecurity. Every fourth respondent claims to be uninformed.

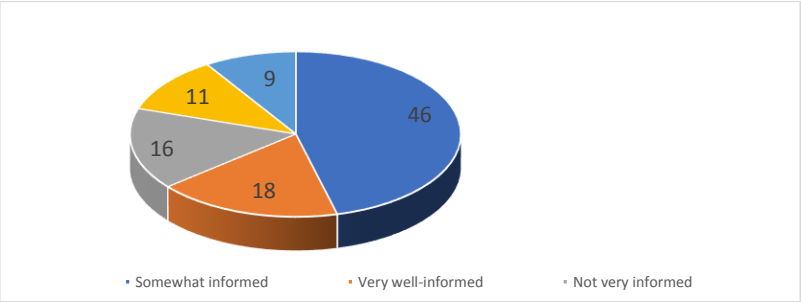

Figure 2. How do they feel about cybersecurity?

Source: Own study based on: (Consumers' Awareness, 2019).

Every fourth respondent realizes that they do not do everything to ensure their safety (25%). Most see their own activity gap (55%), indicating that they could do more to ensure security, while justifying their attitude with the inconvenience of implementing systems and applying security procedures (55%). These inconveniences, in the subjective opinion of the respondents, are so great that they effectively prevent them from taking action, even if their undertaking would be combined with perfect protection (59%). As a result, the cost-benefit ratio is not attractive to the customer, and therefore does not correlate with the customer's net worth. As a consequence, this means that the client, guided by his own criteria, estimates the level of risk acceptable to him.

According to the research, respondents feel vulnerable to cyberattacks, and therefore defenseless in three areas: community (33%), electronic banking (25%) and online shopping (23%). However, it should be noted that Although nearly one-third (32%) of this year's respondents have had a personal credit or debit card compromised, the number has dropped since 2017. At that time, nearly three-fifths (57%) of consumers reported a compromise to a credit or debit card. In the opinion of the respondents, the most valuable information for them, the acquisition of which would be particularly negative for them, is related primarily to: medical documentation (33%), photos (22%) and financial resources (17%).

It is also worth noting that in 2017, 26% of respondents declared cash payments for purchases from their preferred supplier due to the fact that they had suffered a security breach. Two years later, this share increased to 40%. As a result, it can be concluded that a breach of transaction security does not change trust in the bidder, but it results in a change in the way the transaction is performed. However, their declared behaviors differ in the case of hacking social networking sites. They are no longer tolerant and as many as 95% indicate that they would delete the media account if the platform was compromised.

In the context of the discussed issue, interesting observations are also provided by the results of research characterizing the behavior of respondents relating to security in the network (Figure 3).

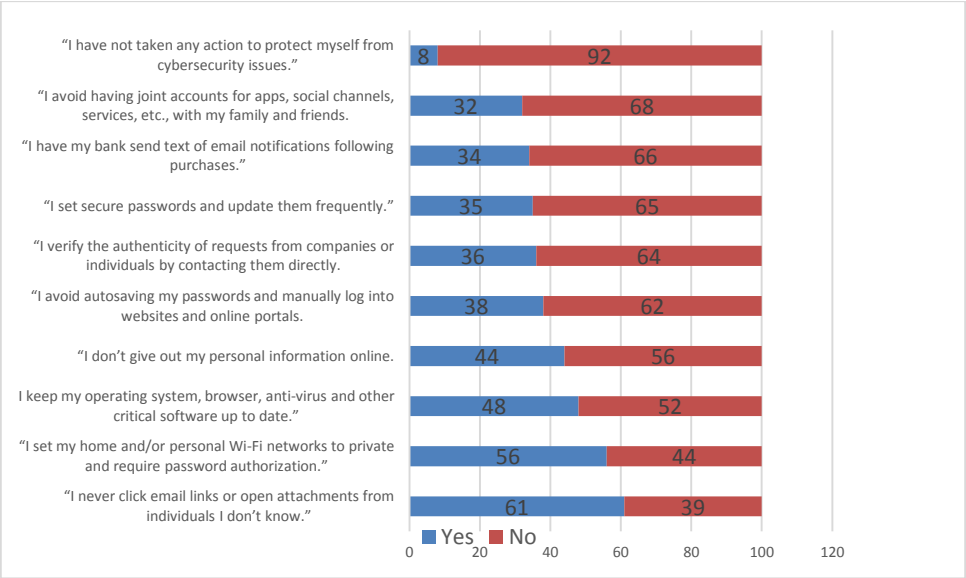

Figure 3. Actions to secure information security.

Source: own study based on: (Consumers' Awareness, 2019).

Most respond correctly by not opening emails with links or attachments from strangers, secure their home or personal Wi-Fi with a private password, but less than half: take care of the operating system, anti-virus software and constant updates, do not disclose their personal information on the Internet, avoids automatic saving of passwords, avoids having shared accounts. Almost every tenth respondent did not take any actions related to the protection of their cyber security. Despite warnings that simple passwords, including passwords containing the names of pets, were often considered weak, as many as 25% use such passwords.

Research indicates differences between the declared and actual digital awareness of the client, ow. More than half say they are taking steps to reduce the risk of a cyberattack. However:

- few change passwords unless forced to (42%).
- they have a "basic password" which they modify slightly to meet certain password requirements (33%).
- would use a public Wi-Fi network that is not password protected, even for sensitive tasks (35%). Only 19% of respondents would never do it, and 28% declare that they would use such a network for online shopping.

The presented research results became the basis for identifying five types of consumer personality, whose characteristics can be related to the awareness of the potential of the network based on the triad: perception, action, knowledge (Table 2).

Table 2.
Personality types in the context of the PAK triad

Personality types	% of respondents	Perception of threats	Action	Knowledge
"Rebellious Olivia"	1	He doesn't understand the importance of cyber security	He doesn't protect himself from it	He doesn't know how to protect himself
"Meticulous Maik"	6	He knows the dangers	He actively wants to protect himself	He took extra steps to gain knowledge
"Trying Terry"	38	He knows the dangers	He actively wants to protect himself	He doesn't have all the information to protect himself, but he's working on improvements
"Ambivalent Endi"	44	He knows the dangers	He will protect himself from it when it is convenient for him	He doesn't worry enough to do anything to protect his data
"Denying Dan"	11	Is somewhat aware of the risks	Does not work to protect itself	Maybe he knows how to protect himself, but he thinks, "there's no way this is going to happen to me"

Source: own study based on: (Consumers' Awareness, 2019).

So, the dominant personality types:

- are aware of cyber security threats,
- take action to protect themselves or declare to take action when it is convenient for them,
- they recognize their knowledge gap and strive to fill it, or they are not concerned enough to take appropriate action.

It is worth noting, however, that respondents realizing the importance of cybersecurity expect tougher cybersecurity measures from companies and the government and believe that both parties could do more (44%).The results of the presented research are also confirmed in Poland (Świadomość Polaków…). It is worth noting, however, that in 2022, compared to 2020, an increase of 182% in the number of cyberattacks was recorded in Poland (Poles in cyberspace, 2022). Despite this high dynamics, in representative research by the company "Procontetnt Communication", only 20% of Poles indicated the experience of an attempted attack understood as a violation of their IT infrastructure at work, data in the home Internet network or theft of funds (Poles in cyberspace, 2022). The results of the report show a serious problem of the lack of awareness of Poles in the sphere of cyber threats.

The cited studies indicate that the experience of a cyber attack is mainly differentiated by age. However, the results presented in Figure 4 do not mean greater susceptibility of young people to such practices, but a greater ability to recognize them. As a result, as the authors of the report indicate, the digital awareness of Poles decreases with age. It also changes with the level of their education. Persons with higher education than those with vocational education admitted to being victims of an attack more often.

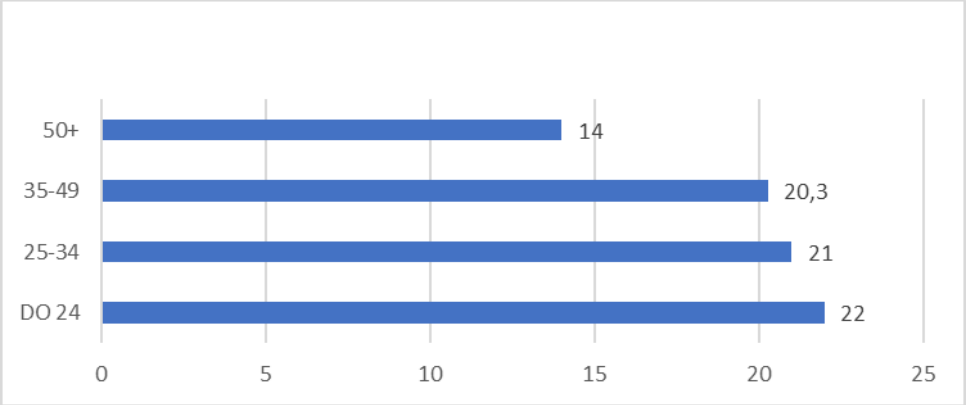

Figure 4. Have you experienced an attempted cyberattack in the last year (yes).

Source: own study based on: (Poles in cyberspace, 2022).

It is also worth noting that 24.1% of respondents indicate a high level of security in the companies they work for, while 11.8% indicate that it is low. Digital trust in individual sectors also varies (Figure 5).

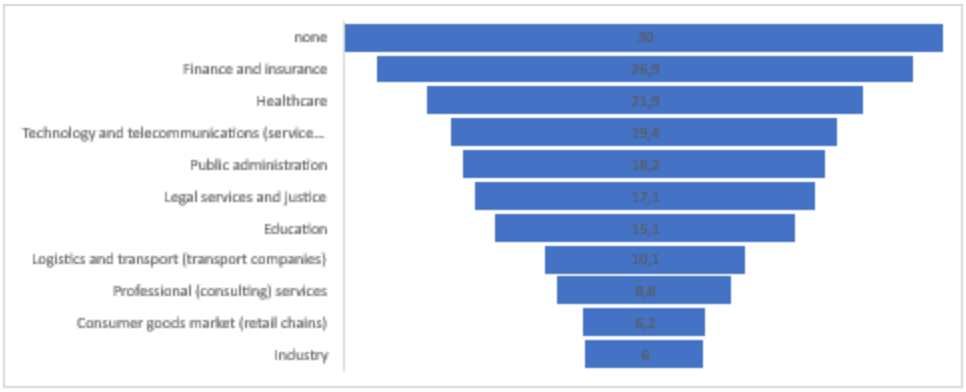

Figure 5. Which of the following sectors do you trust the most when it comes to ensuring the security of your data? (max three indications).

Source: own study based on (Poles in cyberspace, 2022).

It is worth emphasizing, however, that this trust is in contrast to the number of recorded cyberattacks.

The set of the most trusted sectors includes: the financial sector, healthcare and telecommunications, where the largest data breach took place in 2021 (Fig. 5). In the set of sectors that enjoy the least trust, there is logistics, where the smallest number of leaks occurred (Global Threat Report, 2022). These results are also confirmed by the analyzes of Check Point Research, which, taking into account all types of attacks around the world, indicates that the scale of threats in 2022 increased by 28%, and in Poland by 22%. The most frequently attacked sectors in the world are: Education and Research (weekly average of 2,148 attacks - an increase of 18%), Government and military sector (1,564, increase by 1,426), healthcare (1,426 with 60% increase), finance and banking (17% increase) and the wholesale-retail sector (4.4%) (Check Point Research..., 2022).

This may mean, as the authors of the report suggest, that effective image building, through communication with clients, protects the indicated sectors against the loss of credibility. It may also mean that the customer is not aware of the number of leaks and their consequences. Therefore, he builds trust on his own experiences. As a result, it is positive experiences that create his trust. However, the cited studies indicate that most of them cannot recognize cyberattacks and do not identify their consequences. This creates the basis for the statement that consumer's digital trust is also based on irrational premises (imaginations). As a result, a low level of awareness does not preclude high trust.

6.2. The image of online shopping

All cited studies were based on a representative sample, and therefore their results can be confronted with research on consumer attitudes and behavior in the E-Commerce industry (E-Commerce w Polsce, 2022). In the light of the research presented so far, this market enjoyed low consumer confidence and was also vulnerable to cyber attacks. However, it is worth paying attention to the image of the relationship, which is indicated by research on consumer attitudes and behavior in the e-commerce sector (Table 3). The image of this relationship has been positive for years, with a tendency to improve.

Table 3.
The image of online shopping

Years	Rating	Compliance scale					Rating
		1	**2**	**3**	**4**	**5**	
2020	*is complicated/difficult*	2	3	11	27	57	*it is uncomplicated/easy*
2021		2	3	11	27	57	
2022		2	3	10	25	60	
2020	*it is more expensive than buying in traditional stores*	5	5	22	29	42	*it is cheaper than buying in traditional stores*
2021		3	3	21	29	44	
2022		2	4	17	28	48	
2020	*gives less choice of products than traditional purchase*	*2*	*5*	*14*	*23*	*54*	*gives you more product choices than traditional shopping*
2021		3	3	14	21	59	
2022		2	3	10	23	62	
2020	*takes more time than buying in a traditional store*	2	7	16	21	52	*takes less time than buying in a traditional store*
2021		4	6	16	20	54	
2022		4	5	14	20	58	
2020	***IT'S RISKY***	6	12	24	33	26	***IT'S SAFE***
2021		6	11	24	thirty	thirty	
2022		4	9	23	32	32	

Source: Own study based on: (E-Commerce w Polsce 2020-2022).

Therefore, these relationships are perceived as convenient, cheap, fast and, at the same time, safe. As a result, the increase in cybersecurity threats does not affect the perception of relationship security. In general, compared to the previous measurement, the opinion on online shopping is stable, with a slight (statistically insignificant) improvement in all dimensions, regardless of whether the respondent buys online or not. (of course, in this case, the ratings are

lower, but definitely above the middle). Of all the dimensions surveyed, the perception of e-shopping security is relatively the weakest.

These results may suggest that e-customers not so much did not come into contact with cyberattacks, but did not experience their negative consequences. As a result, their experiences have a positive impact on the perception of relationships and trust in this form of shopping. This statement is confirmed by research. Although customers of online stores, when making their choices related to a specific place of online shopping, are guided by many factors, three of them are definitely more important than the others and do not change over the years: attractive product price (47%), low shipping costs/delivery (41%) and previous positive buyer experience (35%).

On the other hand, in the set of factors determining credibility, the following are of key importance: opinions about a given store (43%), the option of cash on delivery (30%) and clear information about returns (29%). It should be emphasized that a significant number of e-consumers are resistant to trust. By using the network in many dimensions, the respondent supports his decision-making process, e.g. when choosing a supplier. 15% of respondents use various websites and portals containing rankings, descriptions and ratings for this purpose. 12% follow friends' recommendations. 12% of respondents review opinions on internet forums. The indicated forms of support for the purchasing process are particularly important for young people (aged 15-24). Opinions on: social networking sites or posted on websites influenced the first choice of the provider for over 17% of respondents in this age group. They are also much more active online.

7. Conclusions

As literature studies have shown, the progressing process of digitization moves business processes to the network, which results in the opening of the customer value creation process. As a result, their course may be influenced not only by the company and the client, but by any entity with access to the Internet and appropriate software.

Therefore, we can talk about a new ecosystem of value exchange, which is evolving along with the ongoing digitization process.

However, it should be emphasized that the new ecosystem of value exchange, based on relationships and interactions, is based on the acquisition, processing and transmission of information. On its basis, knowledge resources are created. The anonymity/invisibility of Internet users calls into question not only the actual knowledge of the information sender, but also his intentions.

In addition, the use of technology whose principles of operation are known and understood by a relatively small group of users may be used for purposes contrary to the user's intentions. This should encourage each user to assess the credibility of information and the safe use of technology. The intensity of information exchange, the increase in the number of users, the dynamic development of complex technologies, indicate the need to create trust resistance in the user.

The legitimacy of taking such actions is also confirmed by the growing problem of cybersecurity.

Supply side of the relationship understands this by implementing and constantly looking for new models of trust.

This side of the relationship is aware that a breach of the security of online relationships, through "data leakage" or depletion of one's own or the other party's financial resources, translates into a decline in reputation. As a result, network security awareness based on the PAK triad encourages the adoption of an attitude of limited trust.

In the light of the cited research, this cannot be said about the e-client. As research has shown, dominant personality types: are aware of cybersecurity threats, take action to protect themselves or declare to take them when it is convenient for them, see their knowledge gap and strive to fill it, or are not worried enough about it to take appropriate action (Table 2). Thus, we are dealing with a gap in the network security potential, which should be reduced, e.g. by providing information to understand the risks of using the Internet to make purchases and to show e-shoppers how they can protect themselves.

The aforementioned gap, however, does not exclude trust (H3.) It can therefore be assumed that trust is a mental state based on rational and irrational premises.

This state is connected with the subjective assessment of the willingness and ability of one party (trusting party) to solve the problem by the other party, made under conditions of risk and uncertainty.

As a consequence, this means that, unlike the company, the client recognizes that creating a state of security is the task of the other party to the relationship. It therefore expects, as research shows, enhanced cyber security measures from companies and the government.

They base their trust on positive experiences rather than actual knowledge. As a result, relationship time becomes a key correlate of trust.

The customer awareness gap is a reflection of the customer experience. So the client has the impression that he is safe. The problem, however, is that a breach of data or information security, in particular, may take place during the purchasing process (gathering information), but it is not necessarily connected with the classic customer-enterprise relationship, and its effects are usually postponed in time. As a result, the customer may experience a cyberattack, but not connect it to the purchasing process. In addition, it should be pointed out that the modern customer participates in the value creation process. So he becomes a co-creator himself. His household is a substitute for an enterprise, all this speaks for him to behave like business units, and thus seek and implement his own model of trust.

References

1. Aarikka-Stenroos, L., Ritala, P. (2017). Network management in the era of ecosystems: systematic review and management framework. *Ind. Mark. Manage., 67*, 23-36. https://doi.org/10.1016/j.indmarman.2017.08.010
2. Accenture, Digital Trust & GDPR: Rethinking the Way Companies can Handle Personal Data (2017). Available at: https://www.accenture.com/gben/about/strategy-index
3. Alsyouf, I. (2007). The role of maintenance in improving companies' productivity and profitability. *International Journal of Production Economics, Vol. 105, Iss. 1,* 70-78. https://doi.org/10.1016/j.ijpe.2004.06.057
4. Bacon, E.C., William, M.D. (2021). *Deconstructing the ivory tower: identifying challenges of university, industry*.
5. Bouncken, R.B., Fredrich, V., Kraus, S., Ritala, P. (2020). Innovation alliances: balancing value creation dynamics, competitive intensity and market overlap. *J. Bus. Res., 112,* 240-247.
6. Caputa, W. (2020). *Customer capital in virtual space*. Warsaw: CeDeWu Publishing House.
7. Caputa, W., Krawczyk-Sokołowska, I., Pierścieniak, A. (2021). The potential of web awareness as a determinant of dually defined customer value. *Technological Forecasting and Social Change, Vol. 163*.
8. Carruthers, P. (2003). *Phenomenal Consciousness. A Naturalistic Theory*. Cambridge: Cambridge University Press.
9. Castelfranchi, C. (2009). A non-reductionist approach to trust. In: J. Golbeck (Ed.), *Computing with Social Trust*. Springer, London Limited, Human-Computer Interaction Series.
10. Castelfranchi, C., Falcone, R. (2010). *Trust Theory: A Socio-Cognitive and Computational Model.* M. Wooldridge (Ed.). Series in Agent Technology. Wiley.
11. *Check Point Research: the number of cyberattacks in the Polish health sector is growing* (2022) https://www.telko.in/check-point-research-rosnie-liczba-cyberatkow-na-polski-sektor-zdrowia
12. Cho, J.H., Chan, K., Adali, S. (2015). A survey on trust modeling. *ACM Comput. Surv., 48, 2, Article 28*, 40. DOI: http://dx.doi.org/10.1145/2815595ACM Computing Surveys (CSUR).
13. Consumers' Awareness (2019). *Behavior and Concerns Around Cybersecurity?* https://merchants.fiserv.com/content/dam/firstdata/us/en/cybersecurity-awareness-insights-study/pdf/FDC_Cybersecurity_and_Awareness_eBook.pdf
14. Delgado-Ballester, E., Manuera-Aleman, J.L. (2000). Brand Trust in the Context of Consumer Loyalty. *European Journal of Marketing, Vol. 35, No. 11/12.* https://doi.org/10.1108/EUM0000000006475

15. Dunn, J.R., Schweitzer, M.E. (2005). Feeling and believing: The influence of emotion on trust. *Journal of Personality and Social Psychology, 88, 5,* 736-748. https://doi.org/10.1037/0022-3514.88.5.736
16. E-Commerce w Polsce (2022), https://gemius.com/api/downloadReport2022.php
17. Fors, A.C. (2010). The beauty of the beast: the matter of meaning in digitalization. *AI & Soc., 25*, 27-33. https://doi.org/10.1007/s00146-009-0236-z
18. Gambetta, D. (1988). Can we trust? In: D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative* Relations (pp. 213-237). New York, USA: Basil Blackwell.
19. Gartner Inc. (2017). *Definition: Digital Trust.* May 4. https://www.gartner.com/en/documents/3727718/definition-digital-trust.
20. Global Threat Report (2022), https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf
21. Horzyk, A. (2012). *Negotiations. Proven Strategies*. Warsaw: Edgard, 1-192.
22. Jackson, M.C. (2000). Systems approaches tomangement. New York: Kluwer Academic Publishers, ISBN 0 306-47465-4
23. Jonek-Kowalska, I. (2012). Ryzyko operacyjne a wartość przedsiębiorstwa na przykładzie przedsiębiorstwa górniczego. *Zeszyty Naukowe Uniwersytetu Szczecińskiego, nr 737, Finanse, Rynki finansowe, Ubezpieczenia, nr 56.*
24. Joyce, S. (2018). Introducing Digital Trust Insights. *Fall 2018. Digital Trust Insights*.
25. Kapoor, R., Lee, J. (2013). Coordinating and competing in ecosystems: how organizational forms shape new technology investments. *Acad. Manage. Proceed., 34(3),* 274-296.
26. Karakuş, I., Kılıç, F. (2022). Digital overview at the profiles of pre-service teachers: Digital awareness, competence and fluency. *Problems of Education in the 21st Century, 80(2),* 324-338. https://doi.org/10.33225/pec/22.80.324
27. Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., Wirtz J. (2021). Corporate digital responsibility. *Journal of Business Research, Vol. 122,* 875-888. ISSN 0148-2963, https://doi.org/10.1016/j.jbusres.2019.10.006.
28. Luhmann, N. (1979). *Trust and Power*. John Wiley & Sons Inc.
29. Najafi, I. (2012). The Role of e-Commerce Awareness on Increasing Electronic Trust. *Life Sci. J., 9(4),* 1487-1494. ISSN:1097-8135. http://www.lifesciencesite.com
30. Ninth Annual Cost of Cybercrime Study (2019). https://www.accenture.com/_acnmedia/accenture/redesign-assets/dotcom/documents/local/1/accenture-ninth-annual-cost-cybercrime.pdf
31. Payne, A.F., Storbacka, K., Frow, P. (2008). Managing the co-creation of value. *J. of the Acad. Mark. Sci., 36*, 83-96. https://doi.org/10.1007/s11747-007-0070-0
32. Pazio, M.N., Formanowska, A. (2002). Struktura świadomości ubezpieczeniowej w świetle badań. *Wiadomości Ubezpieczeniowe, no. 3/4*, 42-43.

33. *Polacy w cyberprzestrzeni – Czy jesteśmy świadomi cyberataków?* https://www.procontent.pl/wp-content/uploads/2022/10/RAPORT-Z-KOMENTARZAMI.pdf
34. Prahalad, C.K., Ramaswamy, V. (2004). Co-creation experiences: The next practice in value creation. *J. Interact*.
35. Rotter, J.B., (1980). Interpersonal Trust, Trustworthiness, and Gullibility. *American Psychologist, Vol. 35, No. 1,* p1_7 Jan.
36. Rouhi, K., Geiger, I. (2023). Management von Marketing-Effektivität und -Effizienz im Einzelhandel: Ein kombiniertes Modell des wahrgenommenen Kundenwerts und des Customer Lifetime Value. In: M. Kleinaltenkamp, L. Gabriel, J. Morgen, M. Nguyen (eds.), *Marketing und Innovation in disruptiven Zeiten*. Wiesbaden: Springer Gabler, https://doi.org/10.1007/978-3-658-38572-9_8
37. Seligman, A.M. (1997). *The Problem of Trust*. New Jersey: Princeton University Press, 43.
38. Swenney, J.C., Soutar, G.N. (2001). Consumer Perceived Value: The Development of a Multiple Item Scale. *Journal of Reatalining, 77*, 203-220.
39. *Świadomość Polaków wobec rzeczywistości cyfrowej.* https://swresearch.pl/raporty/swiadomosc-polakow-w-rzeczywistosci-cyfrowej-bariery-i-szanse-raport-z-badania-bez-komentarzy#report-download,
40. Sztompka, P. (2005). *Sociology of social change*. Krakow: Sign, 70.
41. Szumlicz, T. (2006). Attributes of insurance awareness and foresight. *Ubezpieczenia Dissertations, No. 1,* 21-26.
42. Tadda, G., Salerno, J.J., Boulware, D., Hinman, M., Gorton, S. (2006). Realizing situation awareness within a cyber environment. *Proceedings of SPIE, Vol. 6242 (624204).* Orlando, FL: SPIE.
43. Tripathi, S., Gupta, M. (2021). Indian supply chain ecosystem readiness assessment for Industry 4.0. *International Journal of Emerging Market.* Emerald Publishing Limited, 1746-8809, DOI: 10.1108/IJOEM-08-2020-0983
44. Vargo, S.L., Lusch, R.F. (2011). *It's all B2B and beyond: Toward a systems perspective of the market*. Indium.
45. Vimal, R. (2009). Meanings Attributed to the Term 'Consciousness'. *Journal of Consciousness Studies, 16/5,* 9-27.
46. Williams, P.D. (2008). Security Studies: An Introduction. In: P.D. William. *Security Studies: An Introduction* (pp. 5-10). London/New York.
47. Williamson, O.E. (2014). *The Mechanism of Governance*. New York: Oxford University Press.
48. Wirtz, J., Patterson, P., Kunz, W., Gruber, T., Lu, VN., Paluch, S. (2018). Brave new world: Service robots in the frontline. *Journal of Service Management, 29(5),* 907-931.

49. Yamagishi, T. (2002). *The Structure of Trust: An Evolutionery Game of Mind and Science.* Hokkaido: Hokkaido University Press, 36.
50. Zhang, Z. (2020). Information Security Risk Assessment Based on Cloud Computing and BP Neural Network. *Advances in Intelligent Systems and Computing, 1146*. AISC, 85-91.