NEW EU CYBERSECURITY LEGISLATIONS: CHALLENGES AND RAMIFICATIONS

Huthaifa Albustanji*

1. Introduction

The occurrence and complexity of cyberattacks worldwide, including within the European Union (EU), have been increasing. Cybersecurity risks are constantly changing, with new methods and strategies emerging regularly. Various factors contribute to the rise in cyberattacks within the EU for several reasons like digital Transformation, remote work, sophistication of attacks, IoT Vulnerabilities and inadequate cybersecurity Measures.

To this extent, ensuring cybersecurity has become a significant challenge in the European Union. A considerable number of devices and networks lack adequate security measures, which has raised serious concerns regarding the proliferation of unsecured digital products. In response to these concerns, President Ursula von der Leyen of the European Commission (EC) announced the proposal for the Cyber Resilience Act (CRA). She emphasized the vulnerability of interconnected systems by stating "We cannot talk about defense without talking about cyber. If everything is connected, everything can be hacked"[1]. Consequently, The European Commission suggested revision on Network and Information Security (NIS) directive to raise cybersecurity measures in EU, both legislations are regarded regulatory solutions to combat cyberattack threats[2].

* PHD student, Miskolc University.

1 Munkøe Malthe – Mölder Holger: Cybersecurity in the era of hyper competitiveness: can the EU meet the new challenges. *Revista CIDOB d'Afers Internationals,* Iss. 131., 2022. 69–62.

2 Chiara Pier Giorgio: The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *International Cybersecurity Law Review,* Vol. 3., 2022. 255–273.

Despite the expectation that CRA and NIS2 will be the most efficient regulations for guaranteeing the safety of digital products globally, they pose certain concerns for EU states, manufacturers and customers due the new requirements they introduce. These concerns manifest in various forms, such as the increased cost of highly secure digital products compared to their less secure counterparts. Therefore, this paper aims to critically elucidate the key challenges in the new cybersecurity legislations implemented by the European Union (EU) by exploring the development of EU cybersecurity measures from past to present. Then it will clarify the legal framework of new cybersecurity legislations and finally it will discuss whether customers are willing to pay for cybersecurity or not.

1. The History of cybersecurity measures in EU rules

Ensuring cybersecurity becomes a main target in EU. The absence of adequate cybersecurity in networks and products containing digital components within the union can be attributed to regulatory and market deficiencies. These deficiencies not only pose a threat to the proper functioning of the internal market but also compromise the fundamental rights and safety of individuals[3]. Therefor this section will clarify why enacting legal rules for cybersecurity is necessity and then it will the gradual development of these legislation.

1.1. Justifications for enacting cybersecurity legal rules in EU

The widespread availability of network connectivity enables us to connect with the global community through our computers. However, this connectivity also exposes us to potential unwanted access from the outside world. As data is transmitted, it passes to digital products through multiple physical devices in an encrypted form. The networks that contain digital products is structured into different layers, each with its own vulnerabilities that can be exploited, making cyber-attacks on networks and linked products feasible over the internet[4].

[3] Ibid. 3.

[4] Gagandeep Singh – Vikrant Sharma: Cyber-Security and Its Future Challenges. *International Journal of Information Security and Cybercrime,* Vol. 10., Iss. 1. (2021) 38–50.

Due to the vulnerabilities present in networks, cyber attackers employ various techniques to gain access to data stored in digital products. Their intentions range from breaching this data to tarnishing the reputation of its owner or inflicting financial losses or even for another purposes. The methods employed by these attackers are diverse and encompass ransomware, malware, social engineering threats, and supply-chain attacks... etc. Consequently, the European Union (EU) has initiated the development of frameworks aimed at enhancing cyber resilience, with the objective of mitigating the impact of such attacks**.**

1.2. Beginning of cybersecurity legal framework in EU

The European Union (EU) has been steadily advancing and reinforcing its cybersecurity framework since 2004 with the establishment of the European Union Agency for Cybersecurity (ENISA)[5]. The initial legislation in this domain is the Network and Information Security (NIS) Directive, which became effective in May 2018[6]. The primary objective of the NIS Directive is to enhance the overall cybersecurity level within the EU by compelling member states to adopt a national strategy for securing network and information systems. Additionally, member states are required to appoint national competent authorities to oversee the implementation of this directive. The NIS Directive also imposes specific cybersecurity obligations on critical infrastructure operators in sectors such as energy, transportation, banking, healthcare, and digital service providers. Furthermore, these entities are obligated to report significant cyber incidents to their respective national authorities[7].

The EU Cybersecurity Act 2019 is the second legislation for cybersecurity in the European Union. It was adopted by the European Parliament Plenary in Strasbourg on Tuesday, March 12, 2019, with 586 votes in favor, 44 against, and 36 abstentions. The Act will enter into force 20 days after its publication

5 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

6 Directive 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive").

7 Loan-Cosmin Mihai: Current Challenges in the Field of Cybersecurity. *International Journal of Information Security and Cybercrime,* Vol. 7., Iss. 1. (2018) 9–10.

in the Official Journal of the European Union, once formally approved by the Council[8].

This Act aims to strengthen the European Union Agency for Cybersecurity (ENISA) by providing it with a permanent mandate, increased financial and human resources, and an enhanced role in supporting the EU in achieving a common and high level of cybersecurity. Additionally, the Act establishes the first EU-wide cybersecurity certification framework, which will ensure a unified approach to cybersecurity certification in the European internal market. This framework will ultimately enhance cybersecurity in various digital products and services, including the Internet of Things[9].

Despite the significant contributions made by the NIS directive and EU cybersecurity Act in enhancing cybersecurity measures within the EU, the occurrence of the Covid-19 Pandemic has led to a gradual rise in both the frequency and sophistication of cyberattacks. This has resulted in the identification of numerous vulnerabilities within networks and digital products. Consequently, the necessity to further develop EU cybersecurity has become an undeniable reality. Hence, the subsequent section of this document will elucidate the justifications for amending cybersecurity legal rules.

1.3. Justifications for revision previous cybersecurity in EU

Despite the implementation of EU cybersecurity rules, the onset of the Covid-19 pandemic in 2019 has brought about a significant increase in the utilization of digital applications and products. This surge, driven by the measures implemented by national governments, has unfortunately resulted in heightened vulnerability for individuals and businesses. The pandemic has inadvertently created opportunities for cybercriminals to exploit potential victims by leveraging technologies and messaging platforms. These malicious actors have actively advanced their unlawful techniques through the use of modern

[8] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). See https://tinyurl.com/z4wvb3cr

[9] https://tinyurl.com/2v738rwe

offensive tools. Consequently, the development of cybersecurity measures must keep pace with the evolving nature of these techniques[10].

To this extent, in December 2020 the Council of Europe has acknowledged the growing cybersecurity risks associated with connected devices. It emphasizes the importance of minimizing these risks to safeguard consumers and enhance Europe's cyber-resilience, thereby promoting competitiveness and innovation. The Council has emphasized that cybersecurity and privacy should be considered fundamental requirements in product innovation, production, and development processes, including the design phase (security by design). These aspects should be ensured throughout a product's lifespan and across its supply chain.

EU council found there was a need for improving cybersecurity measures by amending NIS directive; because NIS directive is restricted to specific above-mentioned sectors[11], there is a need for broaden the scope of the current NIS Directive by covering more additional sectors. Furthermore, the broad discretion granted by NIS1 to EU Member States for cybersecurity and incident reporting requirements was seen as excessive, lacking effective supervision and enforcement.

The NIS Directive applies to two distinct categories of organizations: operators of essential services (OES) and relevant digital service providers (RDSPs)[12]. However, it does not extend to public administration services, despite the rising number of cyberattacks targeting such services in various European countries. For example, in Italy alone, there were 13,000 significant cyberattacks on administrative services recorded in 2022, more than double the previous year's figure[13]. It is evident that if the NIS ensured cybersecurity for public services, the number of cyberattacks would not have escalated to such levels. Consequently, the NIS2 Directive mandates that public administration organizations must implement heightened security measures to safeguard sensitive information, including citizens' personal data, financial details, and critical infrastructure data, from cyber threats[14]. In sum, the amendment of NIS

---

10 Lulian Coman – loan-Cosmin Mihai: The Impact of COVID-19 on Cybercrime and Cyberthreats. *European Law Enforcement Research Bulletin – Special Conference Edition,* Iss. 5., 2022. 61–67.

11 Ibid. 8.

12 Ibid. 7.

13 https://www.trade.gov/country-commercial-guides/italy-cybersecurity

14 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation

is crucial for achieving a greater level of harmonization in terms of security requirements and reporting obligations on a boarder level.

2. NIS2 & CRA as advanced frameworks for guaranteeing cybersecurity

EU council has started revision on NIS for the reasons mentioned in the previous chapter. on 3 December 2021, the council adopted its negotiating position compared to the initial proposal for NIS2. Furthermore, on 23 May 2022, the Council has urged the European Commission to propose common EU cybersecurity requirements for connected devices, as well as associated processes and services, by the end of 2022 through the cyber resilience act. The council highlights the necessity for a comprehensive and all-encompassing approach that encompasses the entire lifecycle of digital products, while also taking into account existing regulations, particularly in the field of cybersecurity[15]. Therefore, this section will provide a summary of the key provisions and emphasize the main obstacles linked to the suggested legislations.

2.1. The Network and Information Security 2 directive (NIS2)

In light of the increasing risks brought by digitalization and the rise in cyber-attacks, the European Commission has put forth a proposition on 16 December 2020 for a directive (NIS2) aimed at establishing a high level of cybersecurity throughout the EU. The NIS 2 Directive was published in the Official Journal of the European Union as Directive (EU) 2022/2555[16]. Member States must adopt and publish the measures necessary to comply with the NIS 2 Directive by 17 October 2024.

This directive is intended to replace the existing one and address its limitations. In order to maintain coherence with other relevant EU legislation, the proposal takes into consideration the evaluation of the Resilience of Critical Entities (CER) Directive. The NIS2 proposal seeks to broaden the scope of NIS

(EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

15 https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf

16 Ibid. 15.

by imposing cybersecurity measures on a wider range of entities and sectors, including postal and courier services[17]. Incorporating additional sectors based on their significance to the economy and society. It also establishes a clear threshold, ensuring that medium and large companies in these selected sectors are included within the scope. However, it allows Member States some flexibility in identifying smaller entities with a high security risk profile. The proposal enhances and simplifies security and reporting obligations for companies by implementing a risk management approach, which mandates a minimum set of fundamental security elements. Furthermore, it introduces more detailed provisions regarding the incident reporting process, report content, and timelines. Additionally, the proposal introduces stricter supervisory measures for national authorities, more stringent enforcement requirements, and aims to standardize sanctions regimes across Member States[18].

After the implementation of NIS2, one of the key challenges that arises is the rising expenses associated with cybersecurity measures for organizations; The European Commission has released a projection of the typical growth in ICT expenditure for organizations during the initial three to four years after the implementation of NIS2. For organizations that have newly come under the scope of NIS2, the European Commission anticipates a cost increase of approximately 0.63% of the organization's total turnover. On the other hand, for organizations that are already within the scope of NIS1, the EC estimates a cost increase of 0.58% of the organization's total turnover[19]. The primary additional financial responsibility for businesses will impact the ultimate cost of their goods and services, ultimately resulting in customers paying for highly secure digital products or services.

2.2. Cyber resilience Act (CRA)

Cyber resilience generally refers to the capacity to foresee, plan for, address, and bounce back from cyber-attack. This may encompass a blend of technical safeguards, policies, protocols, and education to safeguard information systems and data against cyberattacks[20]. Cyber resilience involves strategic planning

17 https://tinyurl.com/3c8jsb3j

18 Ibid. 14.

19 Cf. EC, Impact Assessment Report, EU-doc. SWD (2020) 345 final, Part 1/3, 1–96.

20 Alexander Kottigor – Igor Linkov (eds.): *Cyber Resilience of Systems and Networks.* Springer, 2019.

to mitigate risks that may impact an organization's long-term viability. It is designed to minimize operational risks by proactively identifying and addressing cyber threats and incidents before they result in harm. To this extent, EU CRA proposal aims to activate the strategies and techniques to combat cyberattacks on digital products. This section clarifies the general features and challenges of CRA including.

2.2.1. Timeline of CRA proposal

In 2021 and for the purpose of strengthen cybersecurity measures that proposed in NIS2, European commission taking a lead role in cybersecurity and announced the project of a Cyber Resilience Act (CRA) – as a complement to EU's cybersecurity acquis with horizontal cybersecurity requirements for all products with digital elements and the first ever EU- wide law of its kind. The CRA project advanced rapidly and was adopted by EC on 15 September 2022[21]. On December 1, 2023 – A political consensus on the Cyber Resilience Act has been reached by the European Parliament and the Council. The finalized agreement is currently awaiting formal approval from both the European Parliament and the Council. Upon approval, the Cyber Resilience Act will become effective on the 20th day after being published in the Official Journal. Following its enactment, organizations will typically to comply with the updated cybersecurity standards[22].

Once CRA come into force, each Member State would have a period of 36 months to establish a national strategy aimed at safeguarding the resilience of vital entities and conducting periodic risk evaluations under the proposed plan. These evaluations would additionally aid in the identification of crucial entities that would be obligated to enhance their resilience against non-cyber risks. The obligations encompass conducting risk assessments at the entity level, implementing technical and organizational measures, and reporting incidents.

[21] Mira Burri– Zaira Zihlmann: The EU Cyber Resilience Act – an appraisal and contextualization. *Zeitschrift für Europarecht,* 2023/2. 1–28. https://tinyurl.com/ms6apua.

[22] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6168

2.2.2. Features and scope of CRA

The CRA regulations encompass four primary areas. Firstly, they establish guidelines for ensuring the cybersecurity of products that are made available on the digital market by defining their components. Secondly, they outline the requirements that must be fulfilled in the digital design and components of these products, while also considering the responsibilities of digital operators in ensuring cybersecurity. Thirdly, they establish regulations for the vulnerability remediation procedures implemented by manufacturers to ensure cybersecurity throughout the entire life cycle of the product. Lastly, they outline rules for market and manufactures surveillance and compliance with all necessary requirements[23].

CRA determines the scope of application of the law; article 1(a) of CRA states that the CRA applies to 'any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately '. Here the act applies on both hardware and software products. This made ongoing debates regarding whether the regulations are applicable to products that consist of both hardware and software elements, or if they can be applied solely to the software component of such product. For instance, scholar Pier Giorgio Chiara clarifies that the aforementioned principle also applies to software when it is considered as a distinct product from hardware, as indicated by the use of the conjunction 'or'. This is supported by the interpretation of recital 46 of the proposal, which specifically includes products that contain digital components in the form of software. While the legal implications of treating software as a product are beyond the scope of this article, and it is important to explore the extent to which the CRA applies to standalone software[24]. However, CRA excluded several digital products from the scope of its application, it would not apply to products with digital elements that used for medical, automotive[25], aviation[26], national security and military purposes[27]. Furthermore, it excluded software as a service (SaaS),

23 Ibid. 1.

24 Ibid. 3.

25 Art. 2(2) of CRA Proposal, ibid. 1.

26 Art. 2(3) CRA Proposal, ibid. 1.

27 Art. 2(5) CRA Proposal, ibid. 1.

from its application[28]. The proposal suggested theses exception in order to avoid impeding innovation or hindering research in these fields.

2.2.3. The impact of CRA on the cost of digital products

The proposed Cybersecurity Regulatory Authority (CRA) imposes cybersecurity obligations on various economic operators based on their respective roles and responsibilities within the supply chain. Manufacturers are required to ensure that their digital products meet essential cybersecurity requirements and undergo conformity assessment procedures before being made available in the market (horizontal security requirements). Additionally, manufacturers must maintain technical documentation and fulfill notification obligations in the event of cybersecurity breaches[29]. Importers are responsible for introducing only those digital products into the market that comply with essential cybersecurity requirements and display the CE marking[30].

To this extent, manufacturers and importers will be responsible to bear the cost of meeting horizontal security requirements that go beyond their products and at the end of the day, customers will hold the cost once they buy digital products. On the other hand, it is worth noting that many manufactured countries, including China, may not enforce stringent security measures in their digital product markets. Consequently, numerous manufacturers may not prioritize investing in product security[31], but according to the new they cannot exclude themselves from paying on new cybersecurity requirements.

The European commission's executive summary of the impact assessment report on CRA has confirmed the expectation of an increase in the cost of digital products. According to the report, this will result in additional compliance and enforcement costs for businesses, notified bodies, and public authorities[32].

---

28 Art. 9 CRA Proposal, ibid. 1.

29 https://tinyurl.com/y5kjdzan

30 The CE marking serves as a certification mark, signifying compliance with health, safety, and environmental protection standards for products available in the European Economic Area (EEA). It is important to note that the CE marking is not a quality mark, but rather a statement made by the manufacturer, affirming that the product meets the necessary requirements outlined in the relevant European Union (EU) directives.

31 Ibid. 19.

32 Executive summary of the impact assessment report accompanying the document proposal of a regulation for the European parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending regulation (EU) 2019/1020.

These costs will include activities such as notifying, accreditation, and market surveillance. Software developers and hardware manufacturers will also experience higher direct compliance costs due to new cybersecurity requirements, conformity assessment, documentation, and reporting obligations. As a result, the aggregated compliance costs are estimated to reach approximately EUR 29 billion for products with digital elements valued at around EUR 1,485 billion in turnover. End users, including businesses, consumers, and citizens, may consequently face higher prices for products that incorporate digital elements.

The implementation of new laws has impacted the pricing of digital products, as previously discussed. This is just one example of how legal regulations and circumstances can lead to price increases for various products. For instance, in the United States, the Food Safety Modernization Act (FSMA) was put into effect in 2011[33], marking a significant change in the country's approach to food safety. Instead of simply reacting to outbreaks, FSMA focuses on preventing foodborne illnesses by imposing stricter regulations on food producers, processors, and distributors. This shift has brought about a range of consequences for the industry, including higher compliance costs resulting from the authorities' efforts to ensure the safety of these goods[34].

However, it is worth mentioning that CRA and NIS2 mainly focuses on larger organizations such as energy, transport, banking, healthcare, and public administration services infrastructure. However, it also takes into account certain small and medium-sized enterprises (SMEs) that operate in critical sectors or are part of larger supply chains. The reason for including small businesses is that they often face difficulties in implementing advanced cybersecurity measures due to limited financial and human resources. This makes it more challenging for them to comply with cybersecurity requirements[35]. Therefore, the primary effect of these regulations will be felt by large businesses, while smaller businesses will experience indirect consequences due supply chain transformations.

To sum up, this section addressed the primary components of the new cybersecurity regulations in the European Union and the potential economic obstacles that may emerge once they are implemented. It was determined that the responsibility of funding the implementation of these cybersecurity

33 Food Safety Modernization Act, Pub. L. No. 111-353, 124 Stat. 3885 (2011).

34 Aaron Adalja – Erik Lichtenberg: Produce growers' cost of complying with the Food Safety Modernization Act. *Food Policy*, Vol. 74., 2018. 23–38.

35 Ibid. 1., 15.

measures will fall upon the customers of digital products. The question of whether customers typically prioritize investing in improved security has been the subject of extensive discussions. The forthcoming section will further explore these debates.

3. Consumers' willingness to pay for secure digital products

The concept of will to pay (WTP) appeared for the first time over century ago. WTP is described as "an economic value defined as the maximum number of people measurement willing to sacrifice goods and services to obtain other goods and services"[36] .Although there are a few numbers of researches clarifies if customers are willing to pay to get more security such as phishing detection, reducing of digital data theft on digital products. other researches clarified that internet users are not willing to pay for security.

3.1. Peoples' willing to pay for security

Despite lots of customers are not willing to pay by security, many researches and studies declared customers are willing to pay for security of digital products especially if they ensure their extra payment is really reflected on the security of digital products. Generally, EU consumers generally understand the significance of security in upholding stability, prosperity, and the rule of law. They are usually open to financially supporting initiatives that improve their safety and overall welfare. A study conducted by University College London in 2020 regarding the security of 'internet of things' (IoT) devices revealed that consumers are willing to pay extra for increased security, although the specific amount varies based on the device type. Interestingly, the research also indicated that the willingness to pay is not influenced by the extent of risk reduction provided, implying that consumers may not be inclined to pay more for a greater decrease in risk[37].

[36] Rahmat Hidayat – Leni Cahyani – Ratih Hurriyati – Bambang Widjajanta: The Role of Brand Experience in Willingness to Pay: An Online Transportation Case. *Business and Management Research,* Vol. 220., 2021. 326–331.

[37] Market incentives in the pursuit of resilient software and hardware. *National Cyber Security Centre Blog.* https://tinyurl.com/3ht574kf

Another a study conducted by scholar Nguyen et al. (2017) on US customers discovered that consumers are willing to invest in minimizing cyberattacks overall and enhancing online security specifically. To illustrate, in terms of the latter, the research found that users were prepared to pay an additional $9 to $11 per month. Additionally, they were willing to wait an extra 8 to 9 minutes and sacrifice access to 21-29 out of every 100 emails in exchange for improved phishing detection that effectively reduces the influx of spam and phishing emails they receive[38].

Rowe and Wood conducted additional research in the United States to investigate if consumers would be willing to pay for enhanced security measures provided by their Internet Service Provider in order to lower the risks of identity theft and computer malfunctions. The study revealed that, on average, consumers were prepared to pay around $7.24 per month for increased security, resulting in a 16% rise in the average Internet bills in the US[39].

Scholar Dan Svirsky argued in his research "Why are privacy preferences inconsistent" that users are willing to pay considerable amounts of money to get protection on their privacy if the privacy is clearly protected at the time of paying decision making, they prefer to read a stated term for privacy protection in order to increase their confidence[40]. Furthermore Scholar Emami-Naeini in his stated that internet users are to be willing to pay about ten to thirty percent of the base price of a smart device if such data like security and privacy information is given before making a purchase[41].

A recent study carried out by Cyberint Impactful Intelligence revealed consumer sentiments towards cyber threats in the retail and financial sectors. The study indicated that 60% of consumers are inclined to stop shopping with a retailer after a breach, while 83% are contemplating abandoning a financial

---

38 Kenneth D. Nguyen – Heather Rosoff – Richard S. John: Valuing information security from a phishing attack. *Journal of Cybersecurity,* Vol. 3., Iss. 3. (2017) 159–171.

39 Brent Rowe – Dallas Wood: Are Home Internet Users Willing to Pay ISPs for Improvements in Cyber Security? In: Bruce Schneier (Ed.): *Economics of information security and privacy III*. New York, NY, Springer, 2013. 193–212.

40 Svirsky Dan: Why are privacy preferences inconsistent? *Discussion Paper Series publsied in The Harvard John M. Oline Fellow,* Vol. 81., 2018. 1–30.

41 Pardis Emami-Naeini – Henry Dixon – Yuvraj Agarwal – Lorrie Faith Cranor: Exploring how privacy and security factor into IoT device purchase behavior. In: Stephen Brewster – Geraldine Fitzpatrick (eds.): *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems,* Glasgow, SIGGCHI, 2019. 1–12.

app if their data is compromised. Furthermore, 81% of respondents are open to adopting extra security measures[42].

Other researchers discussed found that label that set on digital products which clarifies the security level of them affect the consumer choice and their willing to pay for security[43]. Once customers a security label on the products, they will get more trust of products, and therefore, their conviction for paying on security will be raised. On the other hand, labeling has a positive impact to intensive the industry for fair competition practices.

Indeed, in today's era of digital advancements, it is imperative for customers to acknowledge the significance of investing in security measures. The growing concerns regarding privacy, data breaches, and cyber threats necessitate a willingness to pay for enhanced security. Irrespective of the industry, be it finance, healthcare, or technology, security stands as a fundamental aspect of any product or service. Given the involvement of sensitive information, prioritizing security becomes even more crucial.

3.2. Peoples' unwilling to pay for security

Despite the increased security concerns of digital products in recent years, many individuals are unwilling to pay for security due to various reasons. Certain individuals may hold the belief that the chances of encountering security threats, whether in the digital realm or their immediate surroundings, are highly improbable. This perception of minimal risk can consequently foster the notion that allocating resources towards security measures is superfluous.

Furthermore, customers are often unwilling to pay for security due to a lack of visibility[44]; there are various reasons for this, one being that they may not fully comprehend how their payment is utilized for security measures, because it remains unclear for regular consumers to determine whether their products are truly more secure or not when they pay for security. This lack clear of understanding will lead to reduce in transparency because public sectors failing

42 https://tinyurl.com/nbdrr6d6

43 Shane D. Johnson – John M. Blythe – Matthew Manning – Gabriel T. W. Wong: The impact of IoT security labelling on consumer product choice and willingness to pay. *Plos One,* Vol. 15., N. 1. (2020) 1–21. https://doi.org/10.1371/journal.pone.0227800

44 Wouter de Bruijn – Marco Spruit – Maurits van den Heuve: Identifying the Cost of Security. *Journal of Information Assurance and Security,* 2010/5. 74–83.

to inform regular customers about the repercussions of not implementing robust security measures and how their payments are utilized for security purposes.

Secondly, the lack of awareness is one of these reasons and stems from customers not fully grasping the significance of security measures, which can result in frustration or dissatisfaction with the associated costs. as a result, it can be quite challenging for consumers to make purchasing decisions based on the features of a product, especially when they typically lack knowledge about its internal workings.

Thirdly**,** certain security measures may be viewed as inconvenient or invasive. For instance, the utilization of intricate passwords, activation of two-factor authentication, or undergoing security screenings might be perceived as time-consuming and bothersome**.** Hence, customers opt not to squander their finances and time on security measures.

To this extent, scholars John M., Shane D. and Matthew M. clarified that consumers might show less interest in investing in extra security measures for digital devices that were traditionally considered safe from online threats, like thermostats and watches. However, when it comes to Internet of Things (IoT) products that are connected to physical security, such as security cameras, or to services that are crucial for safety, like thermostats, consumers may be more inclined to pay a higher price[45].

A study conducted by ISACA which is a global professional association and learning organization, revealed that consumers exhibit higher levels of trust when engaging with businesses that employ certified cybersecurity professionals. Certifications remain a crucial aspect in the industry, serving as clear indicators of professionals' expertise, knowledge, and capabilities in the realms of IT and cybersecurity. They play a significant role in showcasing these skills to consumers and stakeholders, thereby enhancing digital trust and confidence in business transactions. Consequently, the report emphasizes that the onus of safeguarding data primarily falls on companies, as most cyberattacks stem from human errors within these organizations. Upon closer examination of the findings, it becomes evident that individuals often overlook investing in security measures because the companies must do that by training their officers on cyber defense procedures[46].

---

[45] John M. Blythe – Shane D. Johnson – Matthew Manning: What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science*, Vol. 1., N. 9. (2020) 1–9.

[46] The Impact of Cybersecurity on Consumer Behavior. *ISACA Now Blog,* 3 October 2022. https://tinyurl.com/mrp6fj5v

3.3. Consequences of non-paying for security

Consumers of digital products are facing challenges in obtaining sufficient security measures at the time of purchasing their digital products, particularly for high-risk items. These challenges arise because governments do not force manufactures to follow such cybersecurity measures before placing their digital products in the market. As discussed in the previous section, many reasons behind non willing to pay for cybersecurity measures set by manufactures. This section will clarify the results of non-paying for more security digital products.

3.3.1. Financial loss

The number of cyberattacks will be increased if high standards of cybersecurity measures have not been followed by manufactures. Ultimately, these cyberattacks will result in financial losses as they have the potential to extort victims or demand ransom. Estimating the precise global damage caused by cyberattacks poses a challenge due to underreporting of incidents.

To this extent**,** the expense associated with a cyberattack can vary for various reasons, such as the magnitude and reach of the attack, the specific organization being targeted, the level of harm inflicted, and the efficacy of the organization's cybersecurity protocols. The financial loss encompasses direct monetary losses arising from theft, fraud, or the identification of network and digital device vulnerabilities. Additionally, it may encompass indirect losses such as the expenses incurred in restoring systems and data, as well as the potential costs associated with blackmail for the return of stolen data.

ENISA, a competent authority, has provided precise statistics on the actual financial losses incurred by several EU countries as a result of cyberattacks. A study reveals that UK companies experience losses amounting to a staggering 37 billion euros annually. Another study highlights that the economic impact can range from 1.01 to 26.19 million euros as an annual cost per company. Additionally, the report mentions that affected companies face costs ranging from 104,000 to 4.35 million euros. Germany, being the second targeted country in the report, experiences losses varying from 425,000 to 20 million euros per company per year, as stated by one of the studies. Lastly, France is also affected

by economic losses ranging from 445,000 to 18.9 million euros per company per year[47].

Furthermore, it could be noted that several cyberattacks have targeted EU companies like FedEx attacks in 2017. in the attacks the criminals targeted the European operations of TNT Express which is a subsidiary of FedEx in June 2017. Theses attack impacted the company's ability to process shipments and caused delays and FedEx reported losses of around $300 million as a result of this attack[48].

Enhancing cybersecurity measures is unquestionably crucial in order to mitigate the high cost of cyberattacks, which has reached billions of euros in various European countries. The expenses associated with cybersecurity measures encompass the procurement and implementation of security software, hardware, and infrastructure, as well as training and education programs. While it's difficult to provide a direct comparison between cybersecurity measures' cost and the cost of a cyberattack, EU governments should aware the citizens of lose occurred as a result of cyberattacks especially that NIS2 and CRA will enter into force in 2024.

3.3.2. Data breaches

The exposure of sensitive data is a frequent outcome of cyberattacks, resulting in various consequences. This includes the compromise of personal information, financial records, intellectual property, and more. Data breaches can have significant impacts on individuals, leading to identity theft and financial fraud. Financial entities, such as banks, are particularly attractive targets for cyberattacks due to the potential for monetary gain and the potential loss of clients if data breaches are discovered. Consequently, it is crucial for all financial entities to utilize the recently provided guidance to identify vulnerabilities in their infrastructure and establish proactive security measures[49].

---

47 The cost of incidents affecting CIIs. Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII). ENISA, 2016. https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis

48 NotPetya cyber-attack cost TNT at least $300m. *BBC,* 20 September 2017. https://www.bbc.com/news/technology-41336086

49 Shields Kristin: Cybersecurity: Recognizing the Risk and Protecting Against Attacks. *North California Banking Institute,* Vol. 19., Iss. 1. (2015) 345–372.

The rise in cyberattacks targeting financial institutions underscores the critical need to protect their data. Consequently, the European Parliament passed the Digital Operational Resilience Act (DORA) on December 14, 2022, to guarantee that the operations of the EU financial sector are capable of enduring operational disruptions and cyber threats. These regulations establish a legal structure for digital operational resilience, requiring all financial institutions to ensure their ability to withstand, respond to, and bounce back from various cyber threats[50].

On the other hand, there was a rise in personal data breaches, with a study revealing that the Netherlands reported the highest number of breaches in Europe from 25 May 2018 to 27 January 2023, totaling around 117,434[51]. Following closely behind was Germany, with over 76,000 personal data breach notifications. The primary reason for this surge in breaches can be attributed to the vulnerabilities present in digital products storing personal data. The implementation of CRA and NIS2 are typical responses to the escalating data breach incidents in the EU.

Data breaches are not the ultimate outcome of cyberattacks; however, they can result in reputational harm by eroding customer trust and confidence, ultimately leading to a decline in business and lasting damage to the organization's brand post-attack. Additionally, companies that do not sufficiently safeguard sensitive data may encounter penalties, legal action, and other repercussions. In the realm of intellectual property, cyberattacks may be directed at businesses in an attempt to pilfer intellectual property, trade secrets, and other valuable assets. Therefore, it is crucial to prioritize the security of digital assets by adhering to cybersecurity protocols outlined in CRA and NIS2.

In sum, cyber-attacks can damage business' reputation and erode the trust customers. This, in turn, could potentially lead to loss of customers, loss of sales, reduction in profits. if businesses unable to safeguard its customers' sensitive data due to a successful cyberattack, that leads to a substantial erosion of trust. According to the IDC, 80% of consumers in developed nations will abandon a business if their data is compromised due to cyberattack. Consequently, this loss of trust prompts customers to opt for competitors who exhibit superior

[50] Regulation (EU) 2022/2554 of the European parliament and of the council of 14 December 2022 on digital operational resilience for the financial sector and amending regulations (ec) no 1060/2009, (EU) no 648/2012, (EU) no 600/2014, (EU) no 909/2014 and (EU) 2016/1011.

[51] Ani Petrosyan: Number of personal data breaches in Europe 2018–2023, by country. *Statista,* Sep. 26, 2023. https://tinyurl.com/9chp6yb9

security measures. the study declared that nearly 60% of businesses ultimately shut down following data breaches[52].

3.4. Raising awareness on paying for cybersecurity

Generally, the notion of awareness described as an understanding arises from the interaction between an entity and its surroundings - in basic terms, being cognizant of the current situation[53]. The significance of maintaining sufficient cybersecurity awareness has been emphasized because the increasing number of cyberattacks in the last years. Therefore, it is crucial to promote cybersecurity practices and foster behavioral and cultural change through educational process starting from children's, youth and old age users.

Cybersecurity awareness pertains to users understanding of cyberattacks and their proficiency in adopting habits to identify and prevent them. To this extent, the landscape of cybersecurity awareness has been continuously developing in reaction to the ever-changing landscape of cyber-attacks. Therefore, EU commission has recognized cybersecurity awareness as one of the most significant challenges in the future due to the increasing number of diverse and sophisticated attacks.

Here, EU has made efforts to raise awareness among its citizens about cybersecurity risks by establishing ENISA as a competent agency for cyber awareness[54]. Additionally, in January 2018, the European Commission (EC) introduced its Digital Education Action Plan with the aim of enhancing digital skills across Europe in order to conduct effective training and awareness-raising activities. This plan includes a specific action (Action 7) dedicated to cybersecurity (COM (2018) 022 final). Action 7 comprises of two key initiatives: firstly, the initiation of a comprehensive EU-wide campaign to raise awareness about cyber culture, promoting online safety, media literacy, and 'cyber hygiene' among children, parents/carers, and teachers. Secondly, the provision of an online and offline course to educate primary and secondary education students

---

52 Matthew Lieberman: Mind The Trust Gap: How Companies Can Retain Customers After A Security Breach. *Forbes,* Dec. 8, 2017. https://tinyurl.com/mryf4pze

53 Eva Nagyfejeo – Basie Von Solms: Why Do National Cybersecurity Awareness Programmes Often Fail? *International Journal of Information Security & Cybercrime,* Vol. 9., Iss. 2. (2020) 18–27.

54 Ibid 6.

about cybersecurity (EC Education and Training n.d.). While these initiatives hold promise, the real challenge lies in their effective implementation[55].

The European Union has made strides in promoting cybersecurity awareness, but there remains a lack of information on the importance of investing more in secure products. Enhancing the Cybersecurity Act (CRA) and the NIS2 directive will require increased efforts to raise awareness among users in the EU cyber market. It would be more effective if NIS2 mandated member states to implement regulations that mandate specific cybersecurity awareness training for employees handling high-risk products. Once these regulations are implemented across the EU, it is anticipated that many citizens will be surprised by the reasons behind the increased costs of digital products. This new cost is expected to have an impact on commercial transactions within the EU digital market.

Investing in cybersecurity awareness is not only an EU mission. At a global scale, there exists a necessity for an international initiative aimed at raising awareness about the importance of investing in cybersecurity measures. Cybersecurity is not only perceived as an economic risk, but also as a threat to individuals' safety as clarified in previous sections[56]. Consequently, the absence of an international organization dedicated to promoting awareness in cybersecurity calls for the implementation of cybersecurity education at all educational levels, including pre-university, university, and post-graduate.

At the end, it's worth mentioning that there are various approaches to promoting cybersecurity awareness, involving both public and private sectors. One highly recommended method is to establish educational programs in collaboration with industry leaders, which effectively promote cybersecurity best practices. A successful example of this is the "Be safe in cyber-space" initiative in Lithuania, where the Lithuanian Communications Regulatory Authority partnered with private companies, the Police, and the Ministry of Interior to raise awareness about cybersecurity among the public[57]. At the end, this kind of initiatives plays a crucial role in addressing cybersecurity awareness if it is applied worldwide, it will help people in combating cyberattacks not only within the country border but the one that transcend national borders[58].

---

55 Wang Faye: Legislative Developments in Cybersecurity in the EU. *Amicus Curiae,* Series 2., Volume 1., Number 2. 2020. 233–259.

56 Kosseff Jeff: Cybersecurity of the Person. *Endment Law Review,* Vol. 17., Iss. 1. (2019) 343–366.

57 Ibid 54.

58 Ibid 8.

4. Conclusion

The research investigates the evolution of cyberattack techniques employed by perpetrators in recent years. The impacts of these attacks have had repercussions on individuals, businesses, and governments in the EU area. Consequently, the European Commission has initiated the drafting of new cybersecurity laws to update existing regulations within the EU. The Cyber Resilience Act and NIS2 directive are scheduled to be implemented in 2024, bringing forth numerous challenges and outcomes upon their enforcement.

The implementation of CRA and NIS2 legislations may face a significant obstacle due to the increasing cost of digital products. This challenge arises from the lack of awareness among customers regarding the importance of investing in highly secure products. The rise in costs could potentially impact economic and commercial transactions within the European Union. Consequently, it becomes imperative to raise awareness about these legislations among customers in the EU market.

The research discovered that the duty of enhancing awareness regarding proposed legislations lies with ENISA, EU member states, competent authorities, the private sector, and civil society. In order to accomplish this goal, it is crucial to foster a culture of cybersecurity through education and research, as well as to create public-private partnerships and cooperation mechanisms. The EU should provide full support to these entities in order to fulfill this mission.

CRA and NIS2 will broaden coverage a wider range of entities and sectors. This extension would require these entities to implement consistent cybersecurity measures, ultimately enhancing Europe's cybersecurity landscape in the foreseeable future. Therefore, this study tackled the impact of these legislation on all new sectors. And the results of the researches are important for end customers and manufactures of digital products as well.

This paper suggests that future research could explore the effectiveness of cybersecurity measures implemented in less developed countries within the EU, in order to assess the global applicability of the EU cybersecurity approach. Additionally, subsequent studies may investigate potential strategies for enhancing cybersecurity at an international scale.