TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance

Mosebolatan Adu

Support of A Secure Open Internet: A Comparative Analysis of the UK and EU Cybersecurity Legislation On Connected Products with Digital Element for SMEs

Master's thesis
Programme Law, specialisation Law and Technology

Supervisor: Dr Agnes Kasper

Tallinn 2023

I hereby declare that I have compiled the thesis independently,
and all works, important standpoints, and data by other authors
have been properly referenced and the same paper.
has not been previously presented for grading.

The document length is 17315 words from the introduction to the end of the conclusion.

Mosebolatan Grace Adu, 05/05/2023
(Signature, date)
Student code: 214160HAJM
Student e-mail address: moseadu@yahoo.com

Supervisor: Dr Agnes Kasper
The paper conforms to the requirements in force.

……………………………………………
(Signature, date)

Chairman of the Defence Committee:
Permitted to the defence
…………………………………
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

The increasing reliance on technology and the use of the Internet in business operations has raised concerns about digital security, particularly for small and medium-sized enterprises (SMEs) in the UK and EU. Cyber-attacks are no longer aimed at big companies for example, governments establishments or international companies but smaller businesses and are now being knockout by cyber attacks, whether directly or indirectly that is why legislative bodies are faced with the pressure of constantly proposing and implementing laws that can reduce or prevent cyber attacks from increasing. The UK Product Security and Telecommunications Infrastructure Bill and the EU Cyber Resilience Act are legislation and proposed regulation, respectively, aimed at improving cybersecurity measures and reducing the risk of cyberattacks. While the UK PSTI bill primarily focuses on digital security, the EU CRA proposed regulation has a broader coverage of cybersecurity measures across different sectors with the aim to bring higher advantages for essential and significant entities in order to enable the process of searching for reliable products.

This research aims to study the current cybersecurity legislation on connected products with digital elements for SMEs businesses in the UK and the EU. The research identifies the problem of digital security and its impact on businesses, including financial losses, reputational damage, and legal liability. The research also highlights the vulnerability of SMEs to cyber threats, with statistics showing that 42% of small businesses in the UK experienced a cybersecurity breach in 2020. The significance of addressing the current problem is to increase awareness and investment in cybersecurity measures among SMEs, protect confidential information, and support an open internet. The research concludes with a structure that familiarizes the reader with the content of the research.

Keywords: Cybersecurity, Digital Element, GDPR, IoT, SME, Telecommunications

INTRODUCTION

The UK and the EU governments have shifted their focus to the Cybersecurity Legislation on connected products for small and medium-sized enterprises (SME) businesses.[1] The section gives a brief overview of the race to have a secure open internet, the cybersecurity legislation in the UK and the EU and how to deal with data theft in these countries. This section mentions the aim of the study and relevant research questions which helps the reader to analyse the purpose of the current study. Moreover, this section highlights the identified problem and the significance of addressing the current problem. Finally, this section ends with the structure of the report that familiarises the reader with the content of the report.

Given its huge implications for the security of online communications and transactions, the open internet notion is extremely pertinent to the debate on cybersecurity. The idea of an open internet is based on the idea that everyone should have unrestricted access to all online material and services. The growth of the internet as a potent instrument for communication, teamwork, and commerce has been largely dependent on this idea.[2] However, since the internet is so accessible, it is also susceptible to a number of cybersecurity risks, such as hacking, phishing, malware, and identity theft.[3] Balancing the demand for an open and free internet with the need to shield people and their data from bad actors is one of the biggest issues in cybersecurity. While cybersecurity safeguards like encryption, firewalls, and multi-factor authentication can aid in reducing these dangers, they can also obstruct access to information and restrict its free flow.[4]

[1] Ponsard, C., Grandclaudon, J., & Dallons, G. (2018). Towards a Cyber Security Label for SMEs: A European Perspective-. ICISSP, 4, 426-431.

[2] Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J. J. (2019). The United Kingdom's emerging internet of things (IoT) policy landscape. *Tanczer, LM, Brass, I., Elsden, M., Carr, M., & Blackstock, J.(2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance*, 37-56.

[3] Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Fatima, Z. (2020). Cyber-attacks in the era of covid-19 and possible solution domains.

[4] Khan, M. J. (2023). Securing network infrastructure with cyber security. *World Journal of Advanced Research and Reviews*, *17*(2), 803-813.

Therefore, having a secure open internet is critical for ensuring that individuals, businesses, and organizations in the UK or the EU can access and share information freely without discrimination and cybersecurity issues. An open internet provides a platform for innovation and creativity, enabling individuals and businesses to develop new products, services, and ideas without unnecessary regulatory barriers.[5] Moreover, an open internet fosters economic growth by creating jobs and driving development in the digital age. It is also important for promoting democracy, human rights, and social justice by enabling freedom of expression and protecting digital rights such as privacy, security, and freedom of speech. Additionally, an open internet provides individuals with access to a broad range of information and knowledge, regardless of their location or socioeconomic status, which is critical for promoting education, research, and lifelong learning. The support of an open internet is essential for ensuring that the internet remains a free and open platform for communication, innovation, and growth in the UK or EU, and for protecting the rights and freedoms of individuals in the digital age.[6]

Most times, consumer-connected devices are with password-protected functions in which the password is easily decoded. This is a known problem as both the UK and EU have been focusing on it.[7] With the constant emerging cyber threats, both the UK and EU have come up with new legislation. The UK and EU initiated the procedure together while the UK was purposely part of the EU, and they have kept on cooperating in keeping large numbers of the general standards aligned. Therefore, presently the Product Security and Telecommunications Infrastructure Bill 2022 (PSTI Bill) is a UK Bill, but it is united to the EU corresponding legislation.[8] So, in December 2022, PSTI Bill was proposed and received a Royal Assent in on December 06, 2022, and will be fully implemented on April 29, 2024. The Bill is divided into two categories, the first part establishes a new regulatory regime to ensure consumer connectable products are safe while the second part deals with the placement and development of mobile, full fibre and gigabit-related networks in the UK.[9] On the other hand, the EU Cyber Resilience Act is a proposed regulation that aims to enhance overall cyber resilience and support cybersecurity for connected products in the

[5] Ponsard, C., Grandclaudon, J., & Dallons, G. (2018), *supra nota* 1.

[6] Zachariadis, M., & Ozcan, P. (2017). The API economy and digital transformation in financial services: The case of open banking.

[7] https://www.taylorwessing.com/en/insights-and-events/insights/2023/01/uk-introduces-new-rules-on-the-security-of-connected-products#:~:text=The%20PSTI%20Act%20gives%20the,them%20available%20in%20the%20UK.

[8] https://www.ifsecglobal.com/cyber-security/product-security-and-telecommunications-infrastructure-psti-act-2022-what-does-it-cover/

[9] Parliament, U. K. (2022). Product Security and Telecommunications Infrastructure (PSTI) Bill (2022).

EU. It would create a kind of cybersecurity template for software and hardware products or intended use that involves primarily connecting to a network.[10] One major stand-out that can be found in the two pieces of legislation is their scope. The UK bill primarily focuses on product security and telecommunications infrastructure, whereas the proposed EU regulation is broader in its coverage of cybersecurity measures across different sectors.

Furthermore, cybersecurity has become a major concern for businesses in the UK and EU, especially SMEs. Digital insecurity can occur when certain security measures are not put in place, for example, an individual or group gains unauthorized access to a company's confidential information, such as customer data, financial records, and trade secrets. The impact of data theft can be severe, including financial losses, reputational damage, and legal liability. One major factor that has contributed to the rise of data theft is the increasing use of technology in business operations. As more companies move online and adopt digital systems for storing and processing data, the risk of data theft also increases. Cybercriminals are constantly evolving their tactics and techniques to exploit vulnerabilities in these systems and steal sensitive data. SMEs are particularly vulnerable to data theft, as they often lack the resources and expertise to implement robust cybersecurity measures. According to a report by the UK government, 42% of small businesses in the UK experienced a cybersecurity breach in 2020.[11] This highlights the need for increased awareness and investment in cybersecurity measures among SMEs.

The following sub-headings will discuss other aspects that will be emphasized during research writing:

Problem Statements

Cyberspace is regarded as the core recent society in the UK and EU it has relatively created access to the online platform that has become essential in the present time to keep financial constancy through leading business as well as overseeing everyday way of life requirements.[12] So to have a more protected cyberspace has become a major threat to

[10] European Commission, (15 September 2022). Shaping Europe#s digital Future: Cyber Resilience Act. Policy and legislation. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[11] Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O. T. S., & Vergara, R. G. (2022). A systematic literature review on cybercrime legislation. *F1000Research*, *11*(971), 971.

[12] Sharma, R. Legislation Related to Cyber Crimes in United Kingdom.

businesses in the UK and EU, especially SMEs.[13] The impact of data theft can be severe, and businesses need to take proactive measures to protect their data and systems. The UK and EU have proposed and implemented several legislations to control data theft and improve cybersecurity measures, and businesses need to comply with these regulations to avoid legal and financial consequences.[14] To mention a few of the legislations are as follows:

In the UK, the NIS Regulation was introduced in 2018 to improve cybersecurity measures and protect businesses from cybercrime. UK Electronic Identification and Trust Services (eIDAS) 2016. A regulation designed for Electronic Transactions.[15] Privacy and Electronic Communications (EC Directive) Regulations 2003.[16] This Act gives people certain privacy rights which relate to electronic communication. The Telecommunication (Security) Act which became law in November 2021 is an Act with the primary aim of regulating the UK network security from cyberattacks on mobile carriers,[17] and, the UK PSTI Bill 2022.[18]

In the EU, the General Data Protection Regulation (GDPR), was introduced in 2018.[19] The aim is to strengthen data protection for EU citizens and requires businesses to implement strong security measures to protect personal data. The Cybersecurity Act,[20] NIS Directive (now the NIS2 Directive, which came into force on 16 January 2023).[21] [22] The EU Cybersecurity Competence Centre and the Network of National Coordination Centres for Cybersecurity (which came into force on 28 June 2021) both seek to improve the EU's ability to stop, identify, and respond to cybersecurity events and enhance cooperation

[13] Farelo, N. M. D. A. (2023). *Design of a Security Toolbox: A Framework To Mitigate The Risks of Cyberspace* (Doctoral dissertation).

[14] Le Nguyen, C., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries:'Law on the books' vs 'law in action'. *Computer law & security Review*, *40*, 105521.

[15] https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/#:~:text=The%20UK%20eIDAS%20Regulations%20set,certificate%20services%20for%20website%20authentication.

[16] Harkins, D. (2020). Data Protection & Freedom of Information Policy. *Policy*.

[17] Telecommunication (Security) Act 2021: https://www.legislation.gov.uk/ukpga/2021/31/enacted

[18] Parliament, U. K. (2022), *supra nota* 9.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj, Accessed on 09 May 2023.

[20] 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). Retrieved from http://data.europa.eu/eli/reg/2019/881/oj , Accessed on 15 April 2023.

[21] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from http://data.europa.eu/eli/dir/2016/1148/oj, 15 April 2023.

[22] https://kpmg.com/de/en/home/insights/2023/02/cyber-security-in-the-eu-nis-2-directive-increases-security-levels.html#:~:text=NIS%2D2%20directive%20raises%20common,of%20all%20EU%20member%20states.&text=The%20European%20Union%20is%20strengthening,force%20on%2016%20January%202023.

between stakeholders. These actions will promote interconnected research and development on the subject and aid in the establishment of a stronger cybersecurity sector in Europe. A more recent Act that the EU Commission proposes on 18 April 2023 the EU Cyber Solidarity Act which is aimed at responding to larger cyber attacks. [23] and, the proposed EU CRA.[24]

These are just a few of the legislative initiatives the European Union has taken to address cybersecurity problems. These rules offer a thorough framework for enhancing network and information system security across the EU, encouraging member-state collaboration, and enhancing cybersecurity in key infrastructure sectors. Although, a narrow focus will be based on comparing the cybersecurity legislation on connectible products with digital elements between the UK PSTI Bill and EU CRA during the research writing.

While many businesses struggle to implement adequate cybersecurity measures, as they lack the resources and expertise to do so. This can lead to non-compliance with regulations and an increased risk of data theft. One of the challenges of compliance with data theft acts is the complexity of the regulations. The GDPR, for example, is a comprehensive regulation that requires businesses to implement a range of measures to protect personal data. This can be a daunting task for businesses, especially SMEs, which may not have the resources to dedicate to compliance. Another challenge is the lack of awareness among businesses regarding their obligations under these regulations.[25] Many businesses are unaware of the cybersecurity risks they face and the measures they need to take to protect themselves. This can lead to non-compliance and an increased risk of data theft. Only a select few companies, such as suppliers of critical services and digital services, are now required by EU legislation to take cybersecurity safeguards. Security measures are required under GDPR as well, but solely to protect personal data. The proposed NIS2 Directive proposes to broaden the scope of cybersecurity duties to include public sector organisations and mid-sized firms, who will be obligated to secure their network and information systems. One of the main issues is that many goods and services on the market have built-in security flaws. By implementing security criteria for numerous devices, the proposed

[23] Molly.K. (19 April 2023). EU launches Cyber Solidarity Act to respond to large-scale attacks – EURACTIV.com

[24] Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. International Cybersecurity Law Review, 1- 18

[25] Mihai, I. C., Ciuchi, C., & Petrică, G. (2023). The Latest Challenges in the Cybersecurity Field. In Regulating Cyber Technologies: Privacy vs Security (pp. 1-18).

Cyber Resilient Act (CRA) aims to address this problem. These requirements will apply to manufacturers as well as businesses and organizations in the supply chain, including importers and distributors, who will also be held responsible for ensuring that the products comply with cybersecurity certification requirements.

Research Aims and Objectives

The primary aim of this research study is to study the UK and the EU cybersecurity legislation with a focus on connected products with digital elements and how it may affect the SME's business. In association with the research aim, the following research objectives have been developed:

- To identify the similarities and differences in the UK and EU legal perspectives on the assessment and compliance of cybersecurity requirements.
- To evaluate the compatibility of the UK and EU legal perspectives on the assessment and compliance of security requirements with digital elements.

Research Questions

Based on the research aim and objectives, the following research question has been developed to address the identified research problem of this research study:

RQ: To what extent the UK and EU legal perspectives are compatible with regard to the assessment and compliance of security requirements relating to digital elements?

Rationale and Significance of the Research

The study will highlight how the security requirements for connectible products with digital elements, such as software, mobile devices, navigation systems, etc. can enhance cybersecurity. This compatibility can help businesses identify threats to their data, take appropriate action, and ultimately secure it. Comparing (the UK & EU) the rules that govern how producers, importers, and distributors should behave on the websites or search engines that are used to reach customers. For e-commerce and SMEs, especially in the cross-border setting, this problem will be extremely important.[26] On the one hand, the security regulations for example GDPR, are likely to improve the situation with data thefts (fewer incidences and misuses are anticipated), which might increase customer confidence in online purchasing and service use.[27] Yet, it is also crucial to understand the prerequisites for this and if producers, importers, and distributors must adhere to substantially comparable or divergent legislative frameworks since this would also affect access to one another's markets.

Understanding the legislation of digital security in the UK and the EU is crucial for businesses for several reasons. Firstly, compliance with these regulations is a legal obligation and businesses that fail to comply risk facing legal and financial consequences. Secondly, understanding the legislation can help businesses to identify and manage cybersecurity risks. By knowing their obligations under the law, businesses can take proactive measures to protect themselves from data theft and other cyber threats.[28] Compliance with data theft legislation such as the Regulation (EU) 2018/1725[29], Directive (EU) 2016/680,[30] and GDPR,[31] can also provide a competitive advantage for businesses. Customers are becoming increasingly concerned about the security of their personal data, and businesses that can demonstrate compliance with regulations may be more attractive to customers.[32] Finally, understanding the legislation is also important for businesses that operate internationally, as different regions have different regulations and requirements.[33] By comparing the legislation of product security and telecommunication infrastructure in the UK and the cyber resilient act in the EU, businesses can gain a better understanding of the similarities and differences between the two regions. This can help businesses that operate in both regions to comply with regulations more efficiently and effectively, and can

[26] Mangku, D. G. S., Yuliartini, N. P. R., Suastika, I. N., & Wirawan, I. G. M. A. S. (2021). The Personal Data Protection of Internet Users in Indonesia. *Journal of Southwest Jiaotong University*, *56*(1).
[27] Vilić, V. (2019). Phishing and pharming as forms of identity theft and identity abuse. *Balkan Social Science Review*, *13*(13), 43-57.
[28] De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. International Journal of Law and Information Technology, 30(1), 68-87..
[29] https://edps.europa.eu/data-protection/our-work/publications/legislation/regulation-eu-20181725_en#:~:text=Regulation%20(EU)%202018%2F1725%20of%20the%20European%20Parliament%20and,EC)%20No%2045%2F2001%20and
[30] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680, Accessed on 09 May 2023.
[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, *supra nota* 19.
[32] Lindqvist, J. (2018). New challenges to personal data processing agreements is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things. International journal of law and information technology, 26(1), 45-63.
[33] Vagena, E., & Ntellis, P. (2020). Cybersecurity legislation: Latest evolutions in the EU and their implementation in the Greek legal system. *EU Internet Law in the Digital Era: Regulation and Enforcement*, 239-259.

also help businesses to identify best practices in cybersecurity and data protection. When complying with regulations, SMEs must abide by a number of cybersecurity laws, including the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR).[34] To prevent charges, sanctions, and legal action, adherence to these rules is required. To safeguard the private information of their clients and to guarantee the safety of their networks and systems, SMEs must abide by these rules. SMEs can comply with these rules with the aid of a strong cybersecurity plan that includes frequent security evaluations and compliance audits.[35]

Dissertation Structure

The first section of this research report (the Introduction) provides a comprehensive background of the research subject. For a clear understanding of the research study, the aim, objectives, and questions related to the problem statement are also offered. Furthermore, chapters one and two will provide a review of the literature, where chapter one presents a comprehensive set of discussions regarding the emergence of an open internet in the UK, chapter two will be discussing the UK and EU cybersecurity legislation and chapter three will cover the methodology and outcome of the research which discuss in details, the comparative analysis of the subject matter. The final section is the conclusion, which provides a summary of the study, including the main findings, limitations, and recommendations. The conclusion should also address the aim and objectives of the study and provide suggestions for future research in the area.

[34] https://bluexp.netapp.com/blog/data-compliance-regulations-hipaa-gdpr-and-pci-dss

[35] Ramadhan, N., & Rose, U. (2022). Adapting ISO/IEC 27001 Information Security Management Standard to SMEs.

1. THE EMERGENCE OF AN OPEN INTERNET

The internet has been widely used all around the world by billions of people; the use of the internet has emerged in the last two decades after the rise of computers and social media platforms.[36] Open Internet can be defined as a system that is connected with interconnected links which permit different documents to be connected in a loop, which creates a structure that can be imagined as a web-like structure, this allowed one to move from one document to another easily.[37] The evolution of the emergence of the open Internet can be tracked from the creation of the World Wide Web (WWW) which was developed in the late 1980s and early 1990s. the creator of the world wide web was Tim Berners who was a computer scientist. The open internet can be said as the development of an internet platform that is accessible to everyone, this era does not count the status, social, economic or political factors but is general for everyone. When technology and computers were not common the use of open internet and computers was limited to some individuals or organisations only. However, as can be seen in these recent times devices and technology is so readily available that everyone is connected to the internet and is connected which made easy access to the internet for everyone. The core concept behind the open internet is based on the concept of impartiality, which describes data as equally treated which makes equality and removes the biases such as pushing a website or link against others, by the service providers, which removed the preferences and created equality.[38]

However, the emergence of the internet has played a beneficial role in society that helped in connecting the world, increasing communication that was not so easy in previous times; people can easily communicate and stay connected. Many new industries came into the market because of it and new business models emerged such as social media platforms, e-commerce and online stores that gave rise to marketing and advertising agencies, developing

[36] Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J. J. (2019), *supra nota* 2.

[37] McPherson, S. S. (2009). Tim Berners-Lee: Inventor of the World Wide Web. Twenty-First Century Books.

[38] Krishna, B., Krishnan, S., & Sebastian, M. P. (2022). Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: an institutional trust theory perspective. *Information Systems Frontiers*, 1-29.

websites and other marketing items. On the other hand, there are many challenges as well such as cybersecurity issues and privacy that are being misused by many people and are exploited. However, with the evolution of the internet, it is also necessary to monitor the channels and take out solutions for these issues to that privacy can be ensured.[39]

1.1. The Importance of Cybersecurity for SME Businesses

Cybersecurity is a major problem for businesses of all sizes in the current digital era. Small and medium-sized businesses (SMEs) are particularly at risk from cyber threats because of their lack of resources and subject-matter expertise. SMEs are exposed to a variety of cyber risks, including phishing scams, ransomware, data breaches, and other criminal activity that can seriously hurt their companies. That is why medium and small size enterprises are being attacked more because they are easy targets and their security can be easily compromised as compared to the large organisations who have experts to manage these issues. There are serious consequences such as huge financial losses, the company's reputation can be destroyed, loss of personal data that can lead to loss of customers and trust issues can happen. In the worst case, the closure of a business can also happen which can be the biggest threat to any organisation.

1.2. Conceptual Framework

Conceptual frameworks are derived from different factors and used in providing ideas to researchers for better studying and analysis of the study. It provides a framework that can help interpret the data and give conclusions. However, for the conceptual framework of cybersecurity, some different terms are used in determining the factors of cybersecurity.[40]

Deterrence Concept

[39] Shukla, M., Johnson, S. D., & Jones, P. (2019, June). Does the NIS implementation strategy effectively address cyber security risks in the UK?. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-11). IEEE.

[40] Jeyaraj, A., & Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity: A text analytics approach. *Journal of Organizational Computing and Electronic Commerce*, *30*(4), 361-380.

A frequently applied legal theory in the fight against cybercrime is deterrence theory. The UK's Computer Misuse Act of 1990 is a good illustration of how the government has applied this idea to impose sanctions on those who engage in cybercrime.[41] Unauthorised access to computer systems is illegal under the Act, and the maximum sentence for conviction is ten years in jail. These punishments are severe in an effort to prevent potential attackers from committing cybercrime. In a similar vein, the Investigatory Powers Act of 2016 empowers law enforcement to apply harsher penalties for cybercrime offences that result in serious harm, such as the destruction of vital infrastructure or human casualties.[42] Additionally, the Act gives law enforcement organisations the authority to compile information to stop and identify major crimes, including cybercrime. Deterrence theory is being applied in the context of the EU to combat cybercrime. Organisations that violate data protection standards are subject to stiff fines under the General Data Protection Regulation (GDPR). According to the GDPR, businesses that violate data privacy regulations may be subject to fines of up to 4% of their annual global revenue or €20 million, whichever is larger.[43] Organisations that could be enticed to participate in cybercrime or other unlawful acts involving the misuse of data are discouraged by these penalties.

The Network and Information Systems (NIS) Directive, which obliges providers of fundamental services to take precautions against and respond to cyberattacks, was also established by the EU.[44] This regulation aims to stop cyberattacks on vital infrastructure, such as the energy and water supply. Furthermore, the directive mandates organisations notify the appropriate authorities of any severe events. Although the UK is no longer a member of the EU, it is still a member of the Council of Europe, which has had a major impact on the creation of global legal guidelines for cybercrime. The Budapest Convention, a treaty on cybercrime drafted by the Council of Europe, attempts to harmonise international cybercrime legislation and create a framework for collaboration among law enforcement agencies. Both the UK and EU member states have joined the Convention, indicating a common commitment to employing deterrence theory to combat cybercrime.

[41] Legislation.gov.uk. 1990. “Computer Misuse Act 1990.” Legislation.gov.uk. 1990. https://www.legislation.gov.uk/ukpga/1990/18/contents.

[42] “Investigatory Powers Act.” n.d. GOV.UK. https://www.gov.uk/government/collections/investigatory-powers-bill#:~:text=On%20Tuesday%2029%20November%202016.

[43] Barrett, Catherine. "Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection?" *Scitech Lawyer* 15, no. 3 (2019): 24-29.

[44] Nikolopoulou, Antonia. "The Directive on security of networks and information systems (NIS Directive) from a practical view." (2019).

Due Diligence Concept

According to the notion of due diligence, people and organisations are obligated to make reasonable efforts to protect others from damage. In the context of rules and regulations requiring businesses to take precautions against cyber dangers, this notion may be applied to cybersecurity. For instance, the General Data Protection Regulation (GDPR) mandates that businesses put in place the proper organisational and technical safeguards to secure personal data.[45] The Cyber Essentials programme in the UK is an illustration of how the due diligence idea is applied to cybersecurity. This programme offers a platform for businesses to apply fundamental cybersecurity precautions and receive certification as proof of their attentiveness. In order to comply with the GDPR and other rules, the UK government also offers guidelines to organisations on how to perform risk assessments and put in place the necessary security measures.

The GDPR in the EU is a prime illustration of the cybersecurity due diligence idea.[46] According to the rule, businesses must put in place the proper organisational and technical safeguards to secure customer data or face steep fines. Additionally, organisations in critical infrastructure sectors are required under the Network and Information Systems Directive (NIS Directive) to establish risk management and security procedures to guard against cyber attacks. The legislation in the UK and the EU are intended to motivate businesses to take preventative measures to guard against cyber risks and safeguard personal information. Due diligence theory encourages organisations to deploy proper security measures and lower the risk of cyberattacks by placing the burden of cybersecurity on the organisations themselves.

1.3. Literature Gap

SME businesses may have different experiences and face different challenges when it comes to complying with cybersecurity legislation while maintaining an open internet.[47] That is why

[45] Ollino, Alice. *Due diligence obligations in international law*. Cambridge University Press, 2022.
[46] Yang, Qiang, Yang Liu, Tianjian Chen, and Yongxin Tong. "Federated machine learning: Concept and applications." *ACM Transactions on Intelligent Systems and Technology (TIST)* 10, no. 2 (2019): 1-19.
[47] Kuzmanovic, A. (2019). Net neutrality: unexpected solution to blockchain scaling. *Communications of the ACM*, *62*(5), 50-55.

the research aims to only target small and medium-scale businesses that can help them in overcoming the problems and consequences that can be caused by cybersecurity issues The previous sections emphasise the significance of cybersecurity for SMEs and the regulatory requirements, including the Payment Card Industry Data Security Standard (PCI DSS) and GDPR, that they must adhere to. Studies that particularly look at how these rules affect cybersecurity for SMEs in the UK and the EU have a large void in the research.[48] Studies already conducted on cybersecurity and SMEs are often broader in scope, concentrating on the difficulties SMEs experience in managing cybersecurity risks and the possible repercussions of cyberattacks. For instance, studies have indicated that SMEs are susceptible to cyber-attacks because of their constrained resources, lack of competence, and lack of knowledge of the dangers associated with cybersecurity.[49] In addition, cyberattacks may cause SMEs to incur large financial losses, harm their reputation, and lose the faith of their clients.

Studies that focus on the effect of regulations like PCI DSS and GDPR on cybersecurity for SMEs in the UK and EU are needed. Such studies might investigate the difficulties SMEs encounter in efficiently complying with these requirements as well as the effects compliance has on their cybersecurity posture. Additionally, research should look at how external elements like government assistance and industry alliances affect compliance and SME cybersecurity resilience. Studies that look at the effect of regulatory requirements on cybersecurity for SMEs in the UK and EU have a large vacuum in the literature. Further investigation is required to comprehend how SMEs may successfully comply with rules like PCI DSS and GDPR, the difficulties they have in doing so, and how compliance affects their cybersecurity posture. This will enhance SMEs' cybersecurity resilience and help strengthen the legal frameworks that safeguard them from online attacks.

[48] Alahmari, Abdulmajeed, and Bob Duncan. "Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence." In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, pp. 1-5. IEEE, 2020.

[49] Tam, Tracy, Asha Rao, and Joanne Hall. "The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses." *Computers & Security* 109 (2021): 102385.

2. THE UK AND EU CYBERSECURITY LEGISLATION ON CONNECTED PRODUCTS WITH DIGITAL ELEMENTS[50]

Taking on new technologies, like smart appliances, may mean fundamentally upgrading your current activities to rival more active organizations and serve demanding clients. Nonetheless, those potential opportunities mean dangers. Digitisation implies greater harm.[51] According to Scott Wilson of eFax, he stated that digitisation without security is a catastrophe waiting to happen.[52] Companies need to guarantee that they can defeat the social or cultural hindrances that are keeping down progress, offer the right help, and go with choices that will both protect and futureproof their companies.

The UK and the EU have several legislation for cybersecurity but due to the constant transformation of digitalization, new cybersecurity threats have emerged. Examples are seen in the coronavirus pandemic where most companies had to embrace the remote working system and the Ukraine war which in return both situations have established room for more cybercrime and an adverse effect on cybersecurity.[53] [54] In order to tackle these new threats, the UK and the EU have introduced new legislation which is - the UK Product Security and Telecommunication Infrastructure Bill, which will come into force on April 29, 2024, focuses on protecting networks and infrastructures against problems enabled by employing insecure consumer connectable products[55] and the EU Cyber Resilient Act which was proposed on the 15 of September 2022, aim at focusing on introducing a compulsory cyber security requirement for all digital products.[56] The legislation that is given by the UK and EU regulatory aims in promoting the security of connected products that can include personal information, increasing trust. But on the other hand, business owners are more inclined

[50] https://www.lexology.com/library/detail.aspx?g=d29fa051-c36f-4fb0-9ec8-be2c09711242

[51] Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. *Enterprise Information Systems*, *15*(4), 565-584.

[52] Wilson, S. (2020). The pandemic, the acceleration of digital transformation and the impact on cyber security. *Computer Fraud & Security*, *2020*(12), 13-15.

[53] Dillon, R., Lothian, P., Grewal, S., & Pereira, D. (2021). Cyber security: evolving threats in an ever-changing world. In *Digital Transformation in a Post-COVID World* (pp. 129-154). CRC Press.

[54] Jelinek, T. (2023). Technology Silos of Today or the End of Global Innovation. In *The Digital Sovereignty Trap: Avoiding the Return of Silos and a Divided World* (pp. 19-33). Singapore: Springer Nature Singapore.

[55] https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets

[56] https://products.cooley.com/2023/01/05/medical-devices-and-ivds-fall-outside-the-scope-of-the-proposed-cra-but-for-how-long/

towards the increased cost because of these additional regulations and their implementation, especially in SMEs.

2.1. The UK Product Security and Telecommunications Infrastructure Bill (PSTI)

The purpose of the UK PSTI Bill, which will take full effect on 29 April 2024, has been categorized into two parts, the product security aspect and the telecommunication aspect. This Bill aims to give the state secretary the power to implement and create the security requirements for customer-connected products sold in the UK, such as smartphones and Internet of Things (IoT) devices, as well as to amend the electronic communication code to allow telecommunication companies to have modernised arrangements.[57] These products include those with specific security and performance requirements, whether they are aimed at consumers or professionals, and include things like electrical and electronic equipment, which excludes some things like smart metres, medical appliances, vehicles, and smart charge points but includes connected cameras and audio, smart TVs, smartphones, and baby toys and monitors.[58] Manufacturers and importers of these items are required by the legislation to ensure that they adhere to applicable security and performance standards, as well as to carry out the necessary testing, risk assessments, and statutory requirements. The performance and security aspects of a device, including any cybersecurity features, must also be disclosed by the manufacturer. Clause 1's authority stipulated that there should be no default passwords, a vulnerability disclosure procedure, notification of security flaws, and openness in the timeline for manufacturer-provided security updates.[59] Additionally, the rules provide a legal framework for the PSTI bill's implementation, including the creation of a new Office for Product Security and Standards. Businesses that violate the rules may be subject to penalties or other enforcement actions, such as a maximum penalty fine of 17 million pounds or 4% of the company's global operating sales.[60] However, the other part of the bill

[57] Parliament, U. K. (2022), (PSTI) Bill, *supra nota* 9.

[58] *Ibid.*

[59] Castilho Salgues, I. A. (2020). *The EU Cybersecurity Framework: An evaluation of the Framework's approach in tackling cyberattacks* (master's thesis).

[60] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials, 22*(2), 1191-1221.

emphasises the alterations to the electronic communication code that oversees the privileges of telecommunication companies to mount infrastructure on the land of the UK that will boost the collaborative associations for the instalment and maintenance of updated telecommunication equipment that will ensure the changes in digital infrastructure such as 5G.

The UK government has developed a voluntary code of practice for Internet of Things (IoT) device manufacturers.[61] The code aims to improve the security of connected products by providing guidelines for manufacturers to follow. The code includes 13 guidelines that manufacturers should adhere to, such as ensuring that all passwords are unique and not resettable to a universal factory default and providing a public point of contact for reporting vulnerabilities.[62] The guidelines are designed to help manufacturers build security into their products at the design stage and to encourage the adoption of best practices throughout the supply chain. While the code is voluntary, the UK government encourages IOT device manufacturers to sign up and commit to implementing the guidelines. By doing so, manufacturers can demonstrate their commitment to security and help to build consumer trust in the IOT ecosystem. Overall, the UK IOT Code of Practice aims to improve the security of connected products, protect consumer privacy, and promote the growth of the IOT industry in the UK.[63]

2.1.1. The Significance of the UK PSTI Bill

Overall, the effectiveness of the UK is generally considered to be high.[64] The bill was introduced by the secretary of state for digital, media and sports, Nadine Dorries. As per the bill, the government has applied a strong process for making cyber security stronger but they needed legislation to protect against any kind of harmful activities by cyber criminals and the other part emphasis on the 5G infrastructure that would make connectivity better and that concerns about the rent reduction faced by the landowners in 2017 ECC reform.

[61] DeNardis, L. (2020). *The Internet in everything*. Yale University Press.

[62] Rixhon, P. (2022). New Media Business Models to Emerge from the Internet of Value. *Enabling the Internet of Value: How Blockchain Connects Global Businesses*, 87-102.

[63] Paul, P. K. (2023). Wireless Sensor Network (WSN) Vis-à-Vis Internet of Things (IoT): Foundation and Emergence. In *Computational Intelligence for Wireless Sensor Networks* (pp. 1-16). Chapman and Hall/CRC.

[64] Bhatia, N. L., Shukla, V. K., Punhani, R., & Dubey, S. K. (2021, June). Growing Aspects of Cyber Security in E-Commerce. In *2021 International Conference on Communication information and Computing Technology (ICCICT)* (pp. 1-6). IEEE.

The system is designed to prevent unsafe and non-compliant products from entering the market, and government agencies have the power to take swift action against manufacturers and businesses that break the rules. One of the key features of the UK's product security regulations is the General Product Safety Regulations 2005 (GPSR), which require manufacturers to ensure that their products are safe for consumers to use. This regulation applies to all consumer products, including toys, electronics, and household goods, and requires manufacturers to conduct risk assessments, monitor security standards, and report any security issues to relevant authorities.[65] The GPSR is enforced by the OPSS, which has the power to order product recalls and levy fines on non-compliant manufacturers. In addition to product security regulations, the bill is a good starting point for consumers because it will restrict businesses that do not have an established cybersecurity domain will have to follow strict regulations and comply with the cybersecurity legislation.[66]

Previously, the UK's product safety and metrology regulations have traditionally focused on physical product safety and measurement accuracy. However, the UK is increasing recognition of the importance of cybersecurity in ensuring the security and reliability of products to ensure the security of consumers. The UK government has responded to this by introducing new regulations to address cybersecurity risks.[67] The UK government has given guidelines for manufacturers, distributors and importers on how to design, supply and follow the legislations that are based on the guidelines provided by the government. The guidelines cover topics such as secure data storage, regular software updates, and strong passwords. Another important development of the UK's product security framework includes provisions for cybersecurity. Under this framework, manufacturers are required to conduct risk assessments that consider cybersecurity risks and respond appropriately to address these risks. In addition, the framework includes new powers for regulators to take action against manufacturers that fail to meet cybersecurity requirements, including the power to order product recalls and levy fines. Despite these new regulations, there are still concerns about the effectiveness of the UK's product security and terms of cybersecurity. The effectiveness of the telecommunication infrastructure will help in increasing the connectivity and

[65] Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J. J. (2019), *supra nota* 2.

[66] Zgraggen, R. R. (2019, June). Cyber Security Supervision in the insurance sector: smart contracts and chosen issues. In *2019 international conference on cyber security and protection of digital services (cyber security)* (pp. 1-4). IEEE.

[67] Bocayuva, M. (2021). Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic. *WMU Journal of Maritime Affairs*, *20*(2), 173-192.

communication in the UK network it will also ensure that the landowners are being satisfied.[68] Overall, the bill is effective for the consumers' rights. The manufacturers, distributors and importers will have to make amendments in their processes as per the requirements of the regulation that will help the businesses to be proficient and will increase the awareness and security of the consumers.

2.1.2 Challenges of the UK PSTI Bill

Many challenges can be faced by the UK such as the issue of lack of enforcement resources for cybersecurity-related regulations, which can make it difficult for regulators to ensure compliance. Another issue is the rapidly evolving nature of cybersecurity threats, which can make it challenging for regulations to keep up with new risks and vulnerabilities. Overall, while the UK has made some strides in addressing cybersecurity risks, there is still more work to be done. The government needs to continue to invest in cybersecurity enforcement resources and update regulations regularly to keep pace with emerging threats. In addition, manufacturers should take a proactive approach to cybersecurity and implement best practices to protect their products and consumers from cyber threats

The UK faces several challenges in addressing cybersecurity risks. One of the main challenges is the rapidly evolving nature of cyber threats, which can make it difficult for regulations to keep pace with new risks and vulnerabilities. This can lead to a delay in regulatory response and an increased risk of products being compromised. Another challenge is the lack of resources and expertise among manufacturers, especially smaller businesses, to implement effective cybersecurity measures.[69] This can lead to vulnerabilities in their products, even if they are compliant with regulations, which can be exploited by cyber attackers. Additionally, there is a lack of coordination between different international standards for cybersecurity in products, which can lead to confusion for manufacturers and challenges for regulators in enforcing standards across borders. Finally, there is a need for increased collaboration between regulators, manufacturers, and cybersecurity experts to address cybersecurity risks in products effectively. This requires the sharing of information,

[68] Deepak, G. C., Ladas, A., Sambo, Y. A., Pervaiz, H., Politis, C., & Imran, M. A. (2019). An overview of post-disaster emergency communication systems in the future networks. *IEEE Wireless Communications*, *26*(6), 132-139.

[69] Bhatia, N. L., Shukla, V. K., Punhani, R., & Dubey, S. K. (2021, June), s*upra nota* 64.

expertise, and best practices to ensure that products are designed, built, and maintained with cybersecurity in mind.[70]

2.2 The EU Cyber Resilience Act (CRA)

On the 15 of September 2022, the commission presented a proposal that was based on legislation for the EU CRA, while profoundly focusing on introducing a compulsory cyber security requirement for all digital products. It was considered a long-awaited idea to be implemented.[71] The need for this approach proposal is missioned on ensuring consumer protection with the idea of enhancing practices concerned with operations when compared with previous findings as stated according to ENISA, for example, in the case of Smart airports which endeavour to deliver ideal services in a dependable and sustainable pattern, by making sure that development, proficiency, well-being and security are ascertained.[72] It is also acknowledged for its role played in the reduction of incidents and threats, along with violation of data associated with cybersecurity, while simultaneously boosting the efficiency of transparency and trust of customers towards product selection.

With a predominant aim of imposing obligations on cybersecurity, the measures proposed by the legislation accumulate the need to place all digital products after withstanding through a procedure of assessment. Along with the fulfilment of the demands as per the requirements that further includes an appropriate design, product management, and innovative development concerning the recent and advanced technological trends to incorporate with data privacy measures. The framework proposed by the EU includes various factors that do belong to horizontal legislation, however, mainly focuses on particular dimensions of cybersecurity that revolve around crises management, services, and products.[73] Through this act, certain rules and laws are established to encounter challenges in the cybersecurity stream by presenting the obligation to follow for all the companies in the EU, with a common vision

[70] Badran, H. (2019, June). IoT security and consumer trust. In *Proceedings of the 20th Annual International Conference on Digital Government Research* (pp. 133-140).

[71] Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements, *supra nota* 24.

[72] Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors*, *19*(1), 19.

[73] Schmitz-Berndt, S., & Chiara, P. G. (2022). One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International Cybersecurity Law Review*, *3*(2), 289-311.

and shared vision. They wish to achieve an increase in resilience and to defend themselves from the security threats taking place in the current century, where undoubtedly there is a huge gap in the balance between data transparency and user privacy. Moreover, a cybersecurity attack affecting a single product can have an impact overall organization or even the supply chain sometimes, spreading beyond internal market boundaries. Henceforth, the act seems to prevail over these issues and foster an atmosphere that discourages and demotivates such practices in general.[74]

2.2.1 The Significance of the EU CRA

Where EU has taken some considerable steps to improve resilience and cybersecurity in recent years, including the adoption of the act, however, the effectiveness of these measures is rather difficult to access. Due to the constant evolvement of cybersecurity threats and breaches of privacy, the effectiveness is moreover dependent on several factors that encompass the level of resources devoted to its implementation followed by an approach to suitably acknowledge the threats lying under it.[75] The certification framework established can assist in ensuring the technical qualities of all the products and services offered, where all the services and products are supposed to meet certain criteria of security along with transparency, while also allowing the European citizens to feel empowered, secure, and trusted by the concerned authorities for any new subject for any further procedures.[76]

The EU's CRA also incorporates a contribution towards cost-effectiveness and performance in transparency and advancement in technology.[77] Additionally, to it, this proposal can allow products including digital elements to represent their conformity and can accumulate easily within the internal market, while also simultaneously allowing the products to be subjected to proper assessment processes for detecting even the slightest error existing in them. Its ever-changing, trends and advancements in emerging technologies acclaim the ethical considerations and concerns related to privacy. Its effectiveness also corporates related to interests and cyber diplomacy respectively followed by providing a guarantee of

[74] *Ibid.*

[75] Osula, A. M. (2022). Building Cyber Resilience: The Defensive Shield for the EU. In *Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives* (pp. 179-196). Cham: Springer International Publishing.

[76] *Ibid.*

[77] Car, P., & De Luca, S. (2022). EU cyber-resilience act.

transparency.[78] In the business and commercial context, the CRA can be extensively significant and effective in strengthening the business and its growth in unfavourable conditions followed by maintaining the strategic priorities of businesses and organizations. As cyber operations are concerned with main security threats, such a measure will certainly help in detecting the nature and severity of cyber threats along with the types of systems and assets that are being protected. It helps a business or an organization to reduce the probability of cyber-attacks, along with detecting and responding to cyber threats with incident response capabilities and minimizing the impact of the attack. In addition to it, an effective CRA and measures can enable recovery from cyberattacks, which includes backup, and recovery strategies contributing to minimizing the impact on the performance and operations of the business.

The EU CRA will promote a coordinated response to cyber threats by requiring EU institutions, agencies, and international bodies (for example NIST) to work closely and share information for the implementation of best practices.[79] It will also emphasize the importance of training and awareness raising, for the encouragement of the culture of cybersecurity across the EU when implemented just as the previous legislations, and ensuring that the institutes, bodies, and agencies are equipped to identify and mitigate cyber risks and crimes.[80] The act will furthermore be effective in providing regulation for market monitoring and enforcement, which is supposed to be carried out by designated market monitoring bodies.[81] Similarly, the EU CRA will make sure for the public, that in the phase of design and development, manufacturers increase the security of goods with digital aspects respectively when it is enforced. It will also stress the idea of providing a unified cybersecurity architecture that makes it easier for both hardware and software manufacturers to adopt in comparison with the existing regulation.[82] It also aims to create security features of goods with digital components more transparent and to make it possible for consumers and organizations to implicate such components securely. The act on a general basis aims to

[78] Yoo, J. (2022). Recent Trends in UN Cybersecurity Governance and South Korea-EU Cooperation. In *Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives* (pp. 235-250). Cham: Springer International Publishing.

[79] O'REILLY, P. A. T. R. I. C. K., & Rigopoulos, K. (2022). Fiscal Year 2021 Cybersecurity & Privacy Annual Report. *NIST SPECIAL PUBLICATION, 800,* 220.

[80] Kertysova, K., Frinking, E., van den Dool, K., Maričić, A., & Bhattacharyya, K. (2018). Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks-Study. European Economic and Social Committee: Bruxelles, Belgium.

[81] O'REILLY, P. A. T. R. I. C. K., & Rigopoulos, K. (2022), *supra nota* 80.

[82] Benson, V., Furnell, S., Masi, D., & Muller, T. (2021). Regulation, Policy, and Cybersecurity.

increase manufacturers' accountability by requiring them to offer security assistance along with program updates to fix found vulnerabilities as well as to inform consumers about the cyber security of the digital products and services they buy, use, and avail throughout. The legislation can provide an appropriate and effective unified set of cybersecurity regulations to minimize and eradicate cybersecurity incidents while simultaneously promoting and encouraging consumers' transparency and trust in products encompassing digital components, followed by ensuring greater protection of personal data and privacy.[83] Henceforth, it is regarded as significantly effective and necessary to inaugurate such acts and practices to overcome this ever-increasing challenge of cyber-crimes.

Moreover, on comparing the UK legislation with the EU CRA, the UK tends to have several laws that discuss and address the different aspects of cybersecurity, as per the Redeemed Data Protection Act and the General Data Protection Act. The NIS regulations impose the importance of cybersecurity and incident reporting on operations as compared to the EU Act which is focused on assessment and conformity. The UK allows certain duties to be imposed for the investigation of potential compliance failures and of manufacturers and importers along with considering actions related to importers' and manufacturers' record maintenance, where the law particularly aims to strengthen the country's telecommunication infrastructure, where it includes provisions of 5G networks and removal of high-risk vendors from the country. Followed by taking effective measures for product security and design by implementing best practices for the development cycle including testing and including vulnerabilities discussed with also implicating appropriate security measures.[84]

The EU CRA, preamble point 67, which indeed raises an important issue of third countries and compatibility of product conformity assessments refers to the ability of digital products to meet the criteria, which is profoundly important while considering the nature of the digital economy where it is considered an extensively significant issue for SME, related to cross-border contexts.[85]

[83] Codagnone, C., Liva, G., & de las Heras Ballell, T. R. (2022). Identification and assessment of existing and draft EU legislation in the digital field. *Study for the Special Committee on Artificial Intelligence in a Digital Age (AIDA). Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg*.
[84] Parliament, U. K. (2022), (PSTI) Bill, s*upra nota* 9.
[85] Codagnone, C., Liva, G., & de las Heras Ballell, T. R. (2022), *supra nota* 84.

2.2.2 Challenges of the EU CRA

The EU CRA, which was proposed in 2021, aims to establish a framework for improving the cybersecurity resilience of EU member states and critical infrastructure providers. However, the Act faces several challenges in achieving its goals.[86] One challenge is the lack of harmonization between EU member states in terms of cybersecurity standards and regulations. This can create confusion for critical infrastructure providers, who may struggle to comply with differing regulations in different member states (conformity assessment). It can also make it difficult for regulators to enforce standards consistently across the EU. Another challenge is the risk group and the pace of technological change, which can make it difficult for regulations to keep up with emerging cybersecurity risks. As new technologies are developed, cyber attackers find new ways to exploit vulnerabilities, which can make existing regulations obsolete. A third challenge is the lack of resources and expertise among critical infrastructure providers, especially in smaller member states. This can make it difficult for these providers to implement effective cybersecurity measures, even if they are required to do so by the Act. Overall, while the EU CRA is an important step towards improving cybersecurity resilience in the EU, it faces several challenges that must be addressed if it is to be effective in achieving its goals.[87] Points 67 of the act also acknowledge the challenges that arise when third countries do not have compatible product conformity assessment foundations concerning the EU. To resolve this issue, the EU CRA aims to establish a framework for the certification of cybersecurity, that will also ensure to meet a high level of security requirements. [88]

[86] https://ecs-org.eu/european-cybersecurity-and-resilience-what-challenges-to-create-a-common-framework/

[87] Ludvigsen, K. R., & Nagaraja, S. (2022). The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity Resilience Act. *arXiv preprint arXiv:2205.13196*.

[88] Van den Abeele, E. (2021). Towards a new paradigm in open strategic autonomy? *ETUI Research Paper-Working Paper*.

3 METHODOLOGY AND OUTCOME OF THE RESEARCH: A COMPARATIVE ANALYSIS

3.1 Research Methodology

Research Philosophy

Interpretivism is a philosophical approach that emphasizes the importance of understanding social phenomena from the perspectives of the people who experience them.[89] In the context of the investigation of the support of an open internet and the impact of cybersecurity legislation on SME businesses in the UK and EU perspective, an interpretive approach can help the researcher learn about the UK and EU perspectives and laws about digital security in several ways. First of all, as Scauso (2020) mentioned in his study, interpretivism emphasises the importance of studying the meanings that people attach to their experiences.[90] This means that the researcher can gain a deep understanding of the UK and EU perspectives on digital security by studying how people in these regions think about and talk about digital security. By analysing legal articles, and other qualitative data sources, the researcher can gain insight into the values, beliefs, and attitudes that underpin the UK and EU approach to digital security. This has helped the researcher gain a deep understanding of the UK and EU laws about digital security by studying the social, political, and economic context in which these laws were developed by analysing historical documents, policy papers, and other secondary data sources.

In short, interpretivism is a useful research approach for gaining a deep understanding of the UK and EU approaches to digital security. and help inform the development of more effective

[89] Junjie, M., & Yingxin, M. (2022). The Discussions of Positivism and Interpretivism. *Online Submission*, *4*(1), 10-14.

[90] Scauso, M. S. (2020). Interpretivism: Definitions, trends, and emerging paths. In *Oxford Research Encyclopedia of International Studies*.

and responsive digital security strategies, as well as contribute to a broader understanding of the social and political factors that shape our digital lives. Different studies conclude that interpretivism also emphasizes the importance of reflexivity in research.[91] This means that the researcher is encouraged to reflect on their assumptions, values, and biases, and to take these into account when analysing data and drawing conclusions.

Data Collection Method

Secondary data collection is an important and often preferable approach for qualitative research studies.[92] This is because secondary data provides access to pre-existing information that can be used to inform and contextualize the research findings. It can also be cost-effective and time-efficient compared to primary data collection methods, which involve gathering data directly from sources through methods such as interviews, surveys, and observations.[93] In the case of investigating the support of an open internet and the impact of cybersecurity legislation on SME businesses in the UK and EU perspective, some important and authentic secondary data sources were used to compare the EU CRA with the UK PSTI Bill, like:

- **Official government documents:** These include reports, policies, and legislation documents issued by the UK government, the European Union, and other relevant regulatory bodies.
- **Academic journals and research papers**
- **Online databases and repositories**

The data analysis method that is used in this qualitative research study on the support of a secure open internet while comparing the UK and the EU cybersecurity legislation on connected products with digital elements in SME businesses is based on content analysis.[94]

[91] Alsharari, N. M., & Al-Shboul, M. (2019). Evaluating qualitative research in management accounting using the criteria of "convincingness". *Pacific Accounting Review*.

[92] Ruggiano, N., & Perry, T. E. (2019). Conducting secondary analysis of qualitative data: Should we, can we, and how? *Qualitative Social Work*, *18*(1), 81-97.

[93] Lemon, L. L., & Hayes, J. (2020). Enhancing trustworthiness of qualitative findings: Using Leximancer for qualitative data analysis triangulation. *The Qualitative Report*, *25*(3), 604-614.

[94] Amarasinghe, S. L., Su, S., Dong, X., Zappia, L., Ritchie, M. E., & Gouil, Q. (2020). Opportunities and challenges in long-read sequencing data analysis. *Genome biology*, *21*(1), 1-16.

Content analysis involves identifying patterns or themes within the data that are relevant to the research question or topic of interest.

Research Limitation

The scope of this study is limited to the UK and EU context, and as such, the findings may not be generalisable to other regions or countries. This means that any conclusions drawn from the study may not be applicable beyond these regions.[95] The study is constrained by the fact that cybersecurity legislation and support for the open internet may differ in other countries, and as such, the findings may not be relevant or appropriate elsewhere. Furthermore, the study relies on secondary data collection, which means that the researcher is limited to the data that has already been collected and made available. This could have implications for the quality and reliability of the data, as the researcher may not have access to the most up-to-date or comprehensive information. Additionally, the data may be biased or incomplete, which could limit the validity and reliability of the findings.[96] The use of qualitative research methods in this study may also be a cause for concern, as qualitative research is often criticized for being subjective and prone to researcher bias. This means that the researcher's own beliefs, values, and assumptions may influence the research findings, which could limit the objectivity of the study. The researcher's interpretations of the data may be influenced by their perspectives and biases, which could lead to inaccurate or incomplete conclusions. Overall, the limitations of this study highlight the importance of considering context and methodology when interpreting research findings. While the study may provide valuable insights into the UK and EU context, it is important to recognize that these findings may not be generalizable to other regions or countries, and may be subject to biases and limitations inherent in the methodology used.

3.2 The outcome of the research

3.2.1 Significant of Cybersecurity for SME Business

[95] Akanle, O., Ademuson, A. O., & Shittu, O. S. (2020). Scope and limitation of study in social research. *Contemporary Issues in Social Research*, 105-114.

[96] Wan, Y., Fu, L. H., Li, C., Lin, J., & Huang, P. (2021). Conquering the hypoxia limitation for photodynamic therapy. *Advanced Materials, 33*(48), 2103978.

Cybersecurity is one of the most essential requirements of SME businesses as it is observed that these kinds of small and mid-sized businesses are more vulnerable to getting affected by hackers and online intruders because they have minimal resources for data protection. On the other hand, multinational companies invest a lot of money in ensuring the security of their sensitive data, however, this is not the same with small and mid-sized businesses.[97] Furthermore, it is observed that stealing the sensitive information of the SME can be very critical and this intruder also blackmails these businesses for ransom money or any other illegal demand to retrieve their critical data. It has been observed that cyber threats have increased since 2011 in the entire world this was the time when technology started growing at a good pace and since the last decade, everything is available on the internet. Similarly, such advancements have also allowed hackers and intruders to illegally steal the data of SME businesses and use it illegally.

Based on research in 2021, European SMEs have suffered a 28% minimum of one form of cybercrime. This outcome has made SMEs extremely worried, about 32% of bank accounts have been hacked online and 31% of reported account takeovers due to impersonation or phishing attacks and 29% of spyware, or viruses were reported as well.[98] After analysis of such cyber-attacks and security-related problems in small and mid-sized businesses, it is essential to understand the significance of the cyber security system in SME businesses otherwise the intruders can wind up the business in just one attack.[99] It is observed that data and information are one of the most precious things for businesses to ensure their sustainability and if the data is stolen by a hacker or any other company then they will be left with nothing.[100] There have been reports that a mid-sized cloth brand was doing quite well in the UK.[101] However, the private data of their valued customers were stolen from their databases, and it was kept live on the internet. This sensitive data included the name of the customers, mobile number, address, credit card details and other private information which

[97] Chandna, V., & Tiwari, P. (2023). Cybersecurity and the new firm: Surviving online threats. *Journal of Business Strategy*, *44*(1), 3-12.

[98] European Commission. (May 2022). SMES and Cybercrime. https://europa.eu/eurobarometer/surveys/detail/2280

[99] Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. *Sensors*, *21*(20), 6901.

[100] Wilson, M., McDonald, S., Button, D., & McGarry, K. (2022). It Won't Happen to Me: Surveying SME Attitudes to Cyber-security. *Journal of Computer Information Systems*, 1-13.

[101] Morais, F., Simnett, J., Kakabadse, A., Kakabadse, N., & Myers, A. (2020). ESG in small and mid-sized quoted companies: perceptions, myths and realities.

was leaked on the internet. This resulted because of a loophole in the network security system of the brand. The customers were quite furious when they saw their personal information live on the internet and they sued the clothing brand for not looking after their personal information and sharing it without their consent.[102] Hence, a huge financial loss was experienced by the clothing brand because of a leak in data security and the brand was also shut down as they went bankrupt after all the charges that were imposed on them by their customers.

Other than the above, there are many other cases where data theft has resulted in financial loss and that have also contributed to the shutting down of the business. Moreover, the importance of data security and the consequences of data loss are considered one of the biggest reasons for increasing the market of cyber security systems in the UK and all around the world.[103] The following image displays the estimated size of the cybersecurity business till the end of 2028.

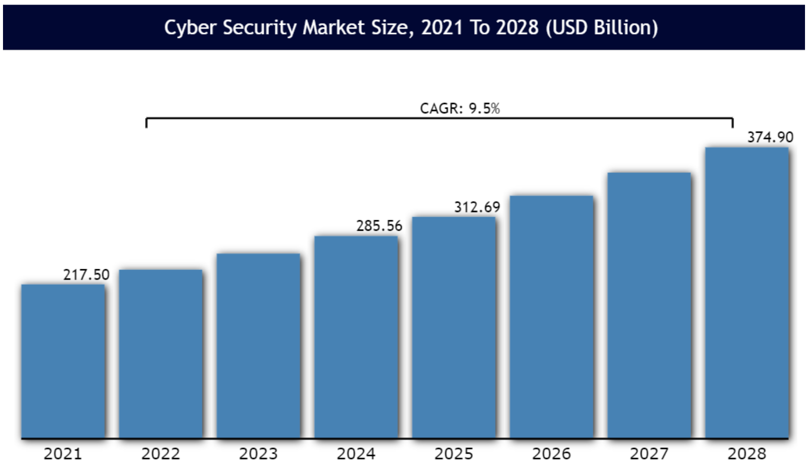


Figure 1. Size of Cybersecurity Market

Source: Lloyd (2020).

The studies show that cybersecurity is one of the main requirements of small and mid-sized businesses and it is essential for any kind of business to ensure that the confidential

[102] Mutalib, M. M. A., Zainol, Z., & Halip, M. H. M. (2021, December). Mitigating Malware Threats at Small Medium Enterprise (SME) Organization: A Review and Framework. In *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)* (Vol. 6, pp. 1-6). IEEE.

[103] Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410.

information of their business and customers are secured professionally which does not allow any intruder to seal any kind of information.[104] It is also observed that sometimes the intruders do not steal the information, but they keep an eye on the data and track the progress of the business which can be used by a competitor company to evaluate the next move of the business. These kinds of threats should also be catered to, otherwise, they can be utilized by the competitors to consider the next move and can also result in a financial loss for the company.[105] Therefore, the graph above shows the jump in the cyber security market because in recent times everything is available on the internet and proper systems and technology are required to assure the security of the data available on the cloud.

3.2.2 Legislation in the UK and EU Regarding Cybersecurity

A cyber security regulation is required to safeguard data technology alongside computer elements to propel different companies as well as organizations to shield their system and data from cyber-attacks.[106] As of today, there have been many clauses and Acts whether proposed or passed by the legislative bodies of different countries which looks after the issues regarding stealing data and other concerns of cyber security. These countries also the European Union have observed the importance of cybersecurity in detail and have passed laws where high penalties are imposed on the people indulging in any kind of cybercrime.[107] The legislation of the UK has introduced different laws where the security of data is defined as one of the most important aspects in the businesses and anyone who tries to steal or tamper with the data without authorisation is considered a crime which can have unpleasant consequences.[108] The Computer Misuse Act was established by the government of the UK in 1990 and is directly connected to the UK's Data Protection Act that was passed in 2018 which aims to protect the personal and valuable data of people from any intruders or

[104] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, *105*, 102248.

[105] Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580.

[106] Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards, and recommendations. *Future generation computer systems*, *92*, 178-188.

[107] Turianskyi, Y. (2020). Africa and Europe: cyber governance lessons.

[108] Singh, H. P., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: a case of Saudi Arabia. *Beijing L. Rev.*, *11*, 637.

hackers.[109] The main idea to introduce these laws was to ensure that modifying or viewing any data without the permission of the owner is considered a legal offence and strict action can be taken against the culprit by the person who owns the piece of information that was tampered with illegally.

It is known that initially in 1990 the Computer Misuse Act[110] was introduced to ensure that the people communicating on the phone calls are end-to-end encrypted and no intruder should be able to hear the conversation between the two people without their consent. This call tampering was quite common in the past in Great Britain where criminals used to hear the conversation on the phone to retain the critical information of the user.[111] However, the phone has become quite secure now and the Data Protection Act established in 2018 primarily aims to reduce the cyber-attack on businesses which has been incorporated into the UK GDPR.[112] Moreover, legislation like Data Protection Act (2018) is important for businesses because it is observed that the maximum cyber threats are reported in the UK and it is considered that the highest density of security issues is found in the UK.[113] This is a concern and laws like Data Protection Act needs to be effectively maintained to ensure that all these crime rates are minimised. Other UK cybersecurity regulations were earlier mentioned in the introduction among them include: The Telecommunication (Security) Act which became law in November 2021 is an Act with the primary aim of regulating the UK network security from cyberattacks on mobile carriers.[114] And to complement the new telecoms security structure, the Product Security and Telecommunications Infrastructure (PSTI) Bill was proposed and received a Royal Assent in on December 06, 2022, and will be fully implemented on April 29, 2024, this bill will deliver much-needed security developments to consumer connectable products.[115]

[109] Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., ... & He, B. (2021). A survey on federated learning systems: vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*.

[110] Child, J. (2021). Computer Misuse Act 1990: CLRNN1: Comparative Report.

[111] *Ibid.*

[112] Quinn, H. (2023). The Information Commissioner's response to the Government's AI White Paper.

[113] Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev.*, 494.

[114] Telecommunication (Security) Act 2021: https://www.legislation.gov.uk/ukpga/2021/31/enacted

[115] https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/telecoms-security-proposal-for-new-regulations-and-code-of-practice

EU on the other hand have several laws in place among them is the Cyber Resilience Act (CRA) which was proposed by the European Commission, the idea of this act was that essential requirements of cyber security should be examined and written on a piece of paper which is called cyber insurance before launching it into the market. This means that it is the responsibility of the manufacturer and developer of the product to ensure that the product is secured from any cyber-attack and that any of the sensitive information will not be modified without authentic authorisation.[116] The following figure shows the increase in cyber insurance after people have understood its importance and it is also helping businesses to get secure from any kind of cyber-attacks.

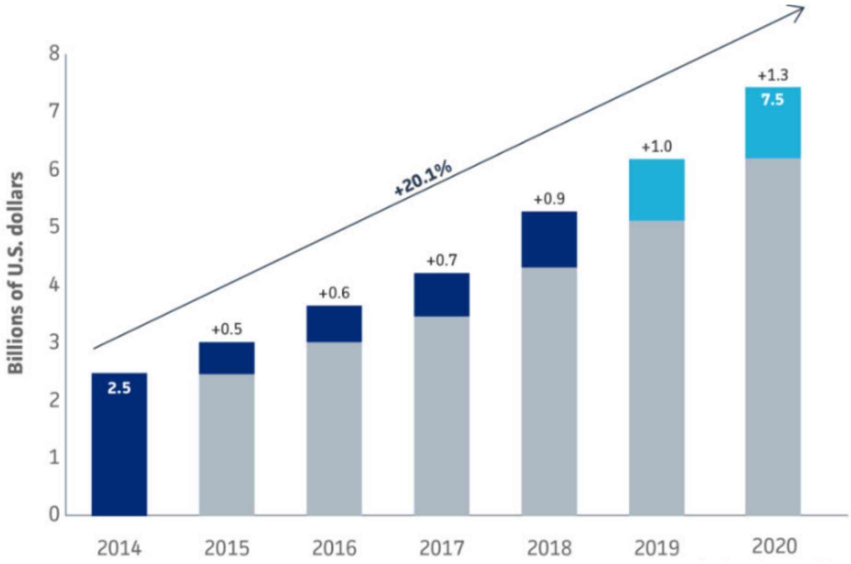


Figure 2. Increase in Cybersecurity Insurance

Source: Sullivan (2021).[117]

It should be noted that different cyber organisations and groups have also been created by the EU members to ensure that cybersecurity is maintained and the cases of cybercrimes are minimised. One of these organisations includes ENISA which is an abbreviation of the European Union Agency for Cybersecurity where the main objective of the agency is to deduce ways which can reduce cyber-attacks or define ways where the hackers can be caught

[116] Zou, B., Choobchian, P., & Rozenberg, J. (2020). Cyber Resilience of Autonomous Mobility Systems: Cyber Attacks and Resilience-Enhancing Strategies. *World Bank Policy Research Working Paper*, (9135).

[117] Sullivan, J., & Nurse, J. R. (2021). Cyber security incentives and the role of cyber insurance. *RUSI Emerging Insights Paper*.

effectively while performing any of these illegal activities so that these activities can be halted.[118] In addition to this, the legislation of the EU has constructed different other agencies for the betterment of data security which includes the European Cyber Security Agency (ESCO) which was established in 2016. Similarly, the European Cybersecurity skill framework defined in ENISA is displayed in the figure below.

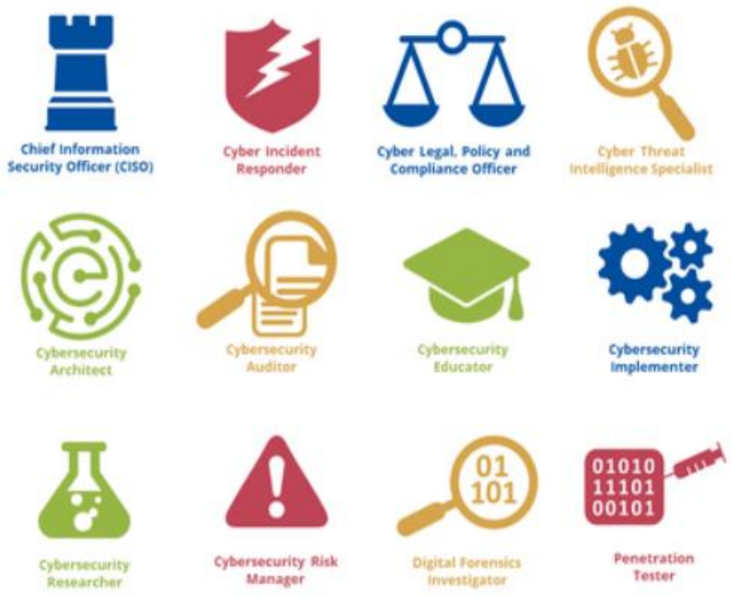

Chief Information Security Officer (CISO)
Cyber Incident Responder
Cyber Legal, Policy and Compliance Officer
Cyber Threat Intelligence Specialist
Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Risk Manager
01
101
Digital Forensics Investigator
01010
11101
00101
Penetration Tester

Figure 3. European Cybersecurity Skill Framework

Source: Nurse, J. R., et.al. (2021).

As shown above, the primary objective of the framework is to establish a main purpose of this framework is to create general considerable knowledge across the EU states basically among companies, people and educational sections, making it an appreciated tool to create a link between the cybersecurity expert organisation and educational environments.[119]

3.2.3 Similarities Between Legislation of the UK and the EU On the Assessment of Cyber security.

The legislation systems of the UK and the EU share several similarities because the main aim of different legislation systems all around the globe is to ensure that the data is secured from

[118] Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity regulation in the European union: the digital, the critical and fundamental rights. *The ethics of cybersecurity*, 97-115.

[119] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

any kind of malicious activity found on the internet. It is assumed that information security is one of the prominent requirements of businesses today and also criminal activities which include modifying and stealing information have increased.[120] The common similarity that can be seen between both of these legislation systems includes establishing different acts and laws to ensure that this sensitive data is secured. On one hand, the European Commission has proposed the Cyber Resilience Act (CRA) which states that any new hardware or software-related equipment should be launched in the market with proper data security elements so that the chances of leaking data from these data are negligible. On the other hand, the legislative bodies in the UK have also passed an act to ensure the data security of its consumers which was termed as Data Protection Act, established in 2018, which states that the stealing or modifying the data without the permission or consent of the authorised user is considered a serious criminal offence and hefty fines can be imposed if anyone is found guilty to this crime which can also lead to imprisonment.[121] For example, for a smartwatch that has a lifetime of 2 to 3 years the security requirement starts getting out of date as the years goes. However, the regulatory bodies and other agencies responsible for the protection of consumer data around the globe have gradually become mindful and at the same time worried about how the software producers and manufacturers of these connectable products have failed to comply with the relevant legal rules [122] (See Chapter 2(10) and (13) of the UK PSTI Bill)[123] and Sec 65 of the EU CRA[124], that is why stringent laws have been put in place for non-compliance which include higher penalty fine in both countries, see Chapter 3(38) of the UK PSTI Bill[125] and Art 53 of the EU CRA.[126]

Another similarity in the legislation for both these countries includes the investments that have been made in dealing with cybersecurity issues. It can be observed in the image above that both countries have been investing a lot of amounts for the betterment of the cyber security systems. Furthermore, it was observed that the problems of cyber-attacks were

[120] Srinivas, J., Das, A. K., & Kumar, N. (2019), *supra nota* 107.

[121] Shukla, M., Johnson, S. D., & Jones, P. (2019, June). Does the NIS implementation strategy effectively address cyber security risks in the UK? In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-11). IEEE.

[122] https://www.wareable.com/health-and-wellbeing/wearable-tech-and-regulation-5678

[123] https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted

[124] Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with Digital element and amending Regulation (EU) 2019/1020. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454 03 May 2023.

[125] *supra nota* 124.

[126] On horizontal cybersecurity requirements for products with Digital element and amending Regulation (EU) 2019/1020, *supra nota* 125.

increasing in the past because people were unaware of the consequences that can be resulted from these cybersecurity issues.[127] In addition to this, the allocation of the budget was also a constraint which resulted in several people losing their important and sensitive information and this was mostly faced by the small and mid-sized businesses because they do not have enough resources to protect themselves from these online thieves and they also do not enough resources to fight against the crime. This has encouraged several online intruders to steal the useful information of innocent people from the internet and then sell it illegally to make money. One more similarity between the legislation system involves the organisation and groups formed by the UK and the EU to ensure minimum and reduction the activities such as leaking information, data theft, modifying the data without authorisation etc.[128] All these problems are identified by these groups and organisations and they tend to reduce these as much as possible.

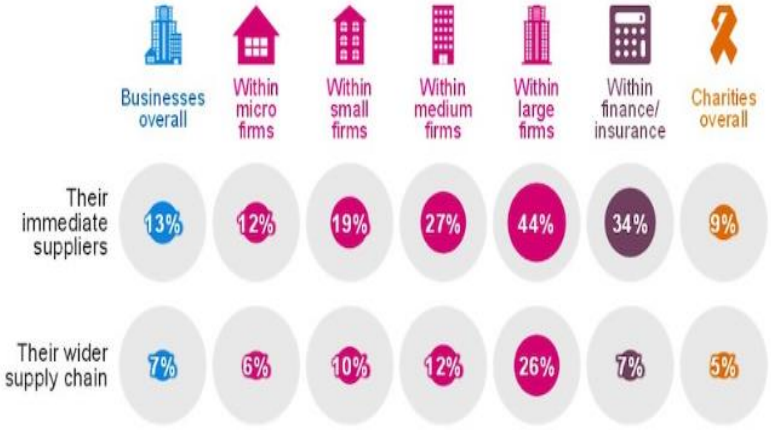


Figure 4. Survey of cyber-attacks on SMEs in the UK and EU

Source: Ponsard, C., & Grandclaudon, J. (2019). [129]

From the figure above, it shows that cyber-attacks are no longer aimed at big companies for example, governments establishments or international companies but smaller businesses and

[127] Onwujekwe, G., Thomas, M., & Osei-Bryson, K. M. (2019, April). Using robust data governance to mitigate the impact of cybercrime. In *Proceedings of the 2019 3rd International Conference on Information System and Data Mining* (pp. 70-79).

[128] Kempen, A. (2019). Cybercrime knows no borders. *Servamus Community-based Safety and Security Magazine, 112*(8), 27-31.

[129] Ponsard, C., & Grandclaudon, J. (2019). Survey and guidelines for the design and deployment of a cyber security label for SMEs. In *Information Systems Security and Privacy: 4th International Conference, ICISSP 2018, Funchal-Madeira, Portugal, January 22-24, 2018, Revised Selected Papers 4* (pp. 240-260). Springer International Publishing.

are now being knockout by cyber attacks, whether directly or indirectly that is why legislative bodies are faced with the pressure of constantly proposing and implementing laws that can reduce or prevent cyber attacks from increasing.[130]

3.2.4 Are there any Differences?

The UK PSTI Bill and the EU CRA are two pieces of legislation aimed at improving cybersecurity. While both laws address similar issues related to cybersecurity, there are many differences between them.

The major difference that can be described between the UK PSTI Bill and the EU CRA is the scope.[131] The UK PSTI Bill focuses on two aspects: product security and the telecommunication infrastructure and possesses fewer security requirements that are required set for the service providers. In contrast, the EU CRA focuses on all the sectors such as the public and private entities. However, a study states that the impact of the EU CRA can affect the energy sector which will have a great influence (positively) on cyber security practices in the energy sector if implemented.[132] This is a result of the previous incidence where there were more than five attacks in a single year including cyber-attacks on the nuclear assets as well.[133] The study also noted that the Act will focus on mandatory requirements as it will be instrumental in driving improvements in cybersecurity. On the other hand, the UK National Cyber Security Centre (NCSC) is a department that focuses on cybersecurity and has examined the cybersecurity risks in the telecommunication centre of the UK. The study focuses on telecommunication by saying that the telecommunication sector was more valued because of its critical role and its link with the internet and communication instruments. Moreover, the study has also recommended that the sector has got minimum security requirements to improve cybersecurity.[134]

[130] *Ibid.*
[131] Zgraggen, R. R. (2019, June). Cyber Security Supervision in the insurance sector: smart contracts and chosen issues. In *2019 international conference on cyber security and protection of digital services (cyber security)* (pp. 1-4). IEEE.
[132] EU Policy Updates - EU Policy Update – February 2023 - CENTR
[133] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN Computer Science*, *3*(2), 127.
[134] Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). Cybersecurity: Legal and Organizational Support In Leading Countries, Nato, And Eu Standards. *Journal of Security & Sustainability Issues*, *9*(3).

Similarly, The EU CRA sets out mandatory requirements for organisations to identify and manage cybersecurity risks. In contrast, the UK sets out minimum-security requirements that must be met by telecommunications service providers.[135] A study by the European Union Agency for Cybersecurity (ENISA) assessed the effectiveness of the Cyber-resilience of Critical Cyber Infrastructures (CCI), this can be compared with the proposed EU CRA if implemented, it will improve cybersecurity.[136] An example is seen in the area of critical cyber infrastructure like health, finance, energy, telecommunication, transportation etc. The main concern here is that these frameworks have become perpetually helpless to cyber attacks, where control frameworks are focused on, as well as encountering information breaks and long-haul invasions.[137] As cyber-attacks are filling in refinement, the outcomes of a single occurrence are expanding in seriousness and bringing about more prominent harm. Disturbances of administrations for example, in any event, for a brief time frame range, can affect the existences of thousands of individuals and fundamentally influence tasks. The study also found that the Act's mandatory requirements will have a positive impact on improving cybersecurity practices and risk management in organizations based on previous incidence.[138] The study also noted that the Act's emphasis on continuous improvement was important in ensuring that organisations remained resilient to cyber threats. Similarly, a study by the National Cyber Security Center (NCSC) examined the effectiveness of minimum-security requirements in improving cybersecurity in the telecommunications sector. The study found that implementing minimum-security requirements had a positive impact on reducing the number of successful cyber-attacks on telecommunications service providers.

Furthermore, The EU CRA will provide penalties for non-compliance with its requirements, including fines and other measures, while the UK sets out a range of enforcement measures that can be used to ensure compliance. According to the report by European Parliamentary, research services, if any business or entity is non-compliance with the law they are at risk of being imposed with fines of 15 million pounds or 2.5% of the yearly turnover from the

[135] Scott, H. S. (2021). The EU's Digital Operational Resilience Act: Cloud Services & Financial Companies. *Available at SSRN 3904113*.
[136] Salvi, A., Spagnoletti, P., & Noori, N. S. (2022). Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, *112*, 102507.
[137] IEC Innovation Report 2019. https://webstore.iec.ch/publication/65943
[138] Oxford Analytica. (2022). EU cybersecurity rules to raise pressure on IoT firms. *Emerald Expert Briefings*, (oxan-db).

overall worldwide operation.[139] In the UK, product security and telecommunication infrastructure fines can be levied on companies and organizations that fail to comply with relevant regulations and standards. Regulatory bodies such as the UK's Office can issue product security fines for Product Safety and Standards (OPSS) for breaches of product safety regulations.[140] These fines can vary depending on the severity of the breach but can be up to £20,000 or unlimited for serious breaches. The OPSS can also issue warnings or recall notices, and in extreme cases, can take legal action against companies that do not comply. Companies and organizations need to take product security and telecommunication infrastructure compliance seriously to avoid fines and other penalties. This helps to ensure the safety and security of products and telecommunications services for consumers and maintains trust in the companies and organisations that provide them.[141]

3.3 Compatibility of the UK and EU Legal Perspectives on Cybersecurity Relating to Digital Elements.

These cybersecurity laws evolved from different legal frameworks that evolved and transformed into the modern perspective. To discuss the compatibility of the UK PSTI Bill and the EU CRA's legal perspectives on cybersecurity relating to digital elements, it is important to first understand the legal frameworks in place. The UK's main legal framework for product security evolved from the General Product Safety Regulations (GPSR) of 2005, which sets out the requirements for the safety of consumer products. The telecommunications sector evolved from the main legal framework the Communications Act of 2003, which regulates the provision of electronic communications networks and services.[142] However, The EU CRA, is a comprehensive legal framework aimed at improving the cyber resilience of EU member states, including their networks and information systems, critical infrastructure, and supply chains. The act introduces new obligations for member states to adopt cybersecurity measures, including risk management, incident reporting, and certification of information and communication technology (ICT) products, services and processes.

[139] Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., & Yu, I. (2021). Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation. *Policy Research Working Paper*, *9594*.

[140] Krüger, P. S., & Brauchle, J. P. (2021). The European Union, cybersecurity, and the financial sector: A primer.

[141] *Ibid.*

[142] Dutton, W. H., Creese, S., Esteve-Gonzalez, P., Goldsmith, M., & Weisser Harris, C. (2022). Next steps for the EU: building on the Paris call and EU cybersecurity strategy. *Available at SSRN 4052728*.

According to the study, the UK PSTI Bill and the EU CRA will have a significant overlap in their legal perspectives on cybersecurity based on previous research.[143] Both the UK and the EU prioritise the safety and security of their citizens' data and digital infrastructure. The EU CRA is aimed at improving the overall cyber resilience of member states and requires suppliers of ICT products and services to obtain certification from approved bodies demonstrating that their products and services meet certain security standards.[144] This requirement is similar to the UK's existing Cyber Essentials scheme, which provides a certification process for businesses that meet minimum cybersecurity standards.

The compatibility of the UK PSTI Bill with the EU CRA is important for businesses that operate across both the UK and the EU, as they need to ensure that their products and services meet the required cybersecurity standards in both regions. In terms of digital elements, the EU CRA places a particular focus on the security of ICT products and services.[145] This includes hardware and software elements, as well as the services that are provided over telecommunications networks. The Act requires that suppliers of these products and services obtain certification from approved bodies, which verifies that the products and services meet certain cybersecurity standards. However, the UK's PSTI Bill also focuses on ensuring the safety and security of digital elements. The Communications Act, for example, requires that telecommunications providers ensure that their networks are secure and that they protect their customers' data. There is a significant overlap between the UK and EU legal perspectives on cybersecurity relating to digital elements, particularly regarding product security and telecommunications infrastructure. Businesses operating across both the UK and the EU need to certify that their products and services meet the essential cybersecurity criteria in both regions and should take action to guarantee compliance with applicable laws and regulations.[146]

[143] Hausken, K. (2020). Cyber resilience in firms, organizations, and societies. *Internet of Things*, *11*, 100204.

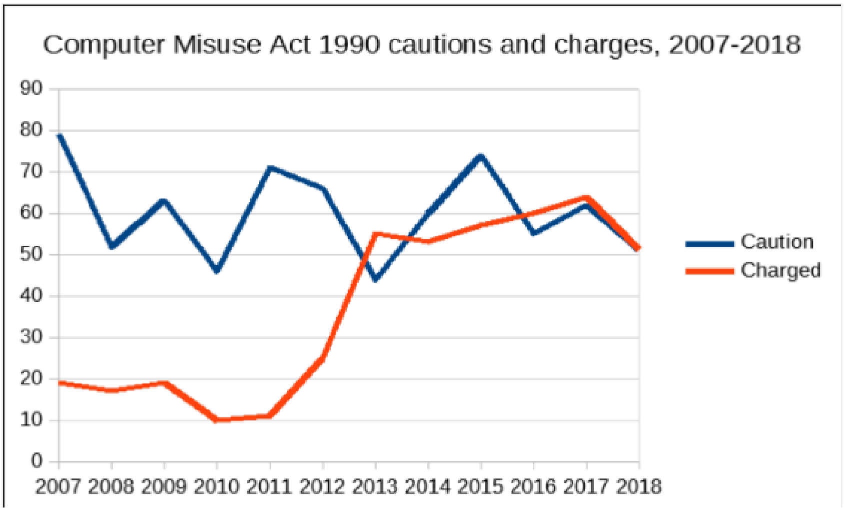
[144] Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements, *supra nota* 24.

[145] *Ibid.*

[146] Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU the example of the financial sector: a legal perspective. *German Law Journal*, *21*(6), 1149-1179.

3.4 Most active Legislation Between the UK and the EU on Cybersecurity

The legislation of both countries has been examined in detail and it is deduced that the policies and acts passed by each of the systems strive to ensure that the data is secured and no one can access the data without proper authorisation. However, after a thorough investigation, it can be deduced that the UK has made stricter laws of cyber security and data theft as compared to the EU and this is also required because the UK can be considered one of the countries with the higher cyber-attacks recorded in a year.[147] In addition to this, it was the UK identified this as a problem back in 1990 when they passed the law called Data Misuse Act 1990 where the idea was to stop intruders from unauthorised access to a computer.[148] The main purpose of the law was to ensure that the phone conversations of people all around the country can be end-to-end encrypted and no outsider can hear the conversation without their permission. This was quite common at that time in the United Kingdom because proper technology was not utilised to ensure the privacy of the phone conversation and hackers were able to find loopholes in the technology.[149] The following graph shows the effectiveness of the Computer Misuse Act that was established in 1990 as it has reduced the number of cases which were reported before of cyber security and data thefts and also the people who are guilty of the crime are charged legally in the court.



[147] Saleem, M. (2019, June). Brexit impact on cyber security of United Kingdom. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-6). IEEE.
[148] Montasari, R., Peltola, P., & Carpenter, V. (2016, June). Gauging the effectiveness of computer misuse act in dealing with cybercrimes. In *2016 International Conference on Cyber Security and Protection Of Digital Services (Cyber Security)* (pp. 1-5). IEEE.
[149] *Ibid.*

Figure 5. Computer Misuse Act 1990 cautions and charges.

Source: Gareth (2019).[150]

Such results show the effectiveness of the law-making and it can be claimed that the laws formulated by the government authorities of the UK are successfully able to reduce cybercrime in the country. On the other hand, laws are also made in the EU to ensure that all the equipment has the essential functionalities to protect the data and ensure cyber security, however, there are no such laws which can caution hackers and intruders to be aware of the consequences before committing any cybercrime.[151] In contrast, the legislation of the United Kingdom has formulated a law to reduce crime which focuses on current data security requirements other than the clauses that were issued in Computer Misuse Act in 1990. This law was introduced in 2018 and it was called Data Protection Act (2018). The sole purpose of the act was to ensure the protection of the data of the people and other organisations that are functional in the country. Also, some of the principles were established in the Data Protection Act which include minimisation of data, credibility and security of data, limiting the storage capacity, permissions to access the information etc. which ensured that the rate of cybercrimes is minimised in the country.[152] It was reported that cybercrimes were quite high in the United Kingdom and it was reported to be 60 per cent in 2017. However, the following image suggests that the rate of cybercrime have been reduced after the Data Protection Act, but the legislation team also needs to take special measure to completely remove it.

[150] Gareth, C. (2019). Guilty of hacking in the UK? Worry not. https://www.theregister.com/2019/05/29/computer_misuse_act_prosecutions_analysis/

[151] Walters, R., & Novak, M. (2021). Cyber security. In *Cyber security, artificial intelligence, data protection & the law* (pp. 21-37). Singapore: Springer Singapore.

[152] Spencer, A., & Patel, S. (2019). Applying the data protection act 2018 and general data protection regulation principles in healthcare settings. *Nursing Management*, *26*(1).

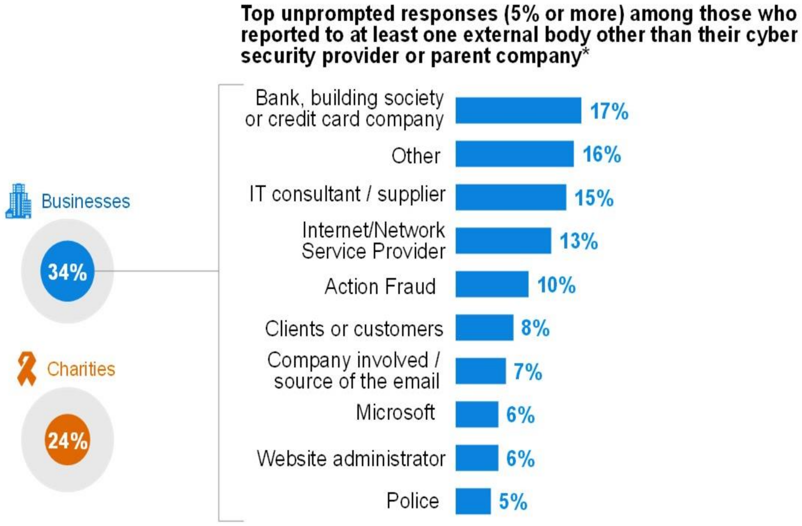


Figure 6. Reduced Cybercrimes in the UK after Data Protection Act

Source: McKeown, J. (2023). [153]

As shown above, the UK government has thought about a methodology to limit outcomes related to cyber security dangers. This methodology is to increase information in regards to capacities of the cyberspace and precluding cyber-attacks and creating arrangements and different techniques for disallowing cyber attacks and making severe moves against cybercrime.[154]

3.5 Non-compliance and less active legislation in the UK and the EU Regarding Cybersecurity

Cybersecurity is an ever-evolving field, and legislation needs to keep pace with technological advancements to remain effective. The acts discussed in the table below have failed to provide adequate protection for individuals' data and online activities, and in some cases, have been criticized for being too intrusive and lacking privacy protections.

The UK Less Active Cybersecurity Legislation

- **The Computer Misuse Act (1990)**

[153] McKeown, J. (2023). A data-driven analysis of UK cyber defence. *arXiv preprint arXiv:2303.07313*.
[154] Sharma, R. Legislation Related to Cyber Crimes in United Kingdom.

This Act was designed to criminalize hacking and other forms of computer-related crime. However, the act has been criticized for being too broad and lacking clarity. This has led to inconsistencies in the way the act is enforced and has made it difficult for prosecutors to secure convictions. Additionally, the act has not kept up with the changing nature of cybercrime, particularly with the rise of cyber espionage and cyber warfare. As a result, the act has been criticized for being outdated and ineffective.[155]

- **Investigatory Powers Act (2016)**

This also known as the ***"Snooper's Charter,"*** was designed to give law enforcement agencies and intelligence services more powers to monitor online communications.[156] However, the act has been criticized for being too intrusive and lacking adequate privacy protections. Additionally, there are concerns that the act could be abused by law enforcement agencies and could have a chilling effect on free speech. A report by the Joint Committee on Human Rights found that the act was "inconsistent with the right to privacy" and recommended that it be amended.

The EU Less Active Cybersecurity Legislation

- **The Network and Information Security Directive**[157]

The EU NIS Directive was introduced in 2016 to improve cybersecurity across the EU internal market.[158] However, the directive has been criticized for being too vague and lacking enforcement mechanisms. Additionally, there are concerns that the directive could lead to overregulation and hinder innovation. A report by the European Union Agency for Network and Information Security (ENISA) found that the directive had been implemented inconsistently across member states and that there was a lack of clarity on certain aspects of the directive.[159]

[155] Howell, C. J. Cybercrime Investigation-Readings. *Murdoch University Electronic Journal of Law*, *8*(2), 2-42.
[156] Wilkinson, S. (2022). UK data protection and digital information bill explained. *Journal of Data Protection & Privacy*, *5*(3), 242-253.
[157] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, *supra nota* 18.
[158] https://eucrim.eu/news/edps-provides-opinion-on-cybersecurity-directive/#:~:text=The%20current%20EU%20Network%20and,functioning%20of%20the%20internal%20market.
[159] Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 105336.

- **Cybersecurity Act (2019)[160]**

There is currently no data on its non-compliance issues. However, there have been concerns raised regarding the act's implementation and its potential impact on businesses operating within the EU. One concern is that the act may lead to overregulation, making it difficult for businesses to comply with the certification requirements. The certification process may also be time-consuming and costly, particularly for SMEs, which could put them at a competitive disadvantage. Another concern is that the act may not be effective in addressing emerging cybersecurity threats, such as those posed by new technologies like artificial intelligence and the Internet of Things. Critics have argued that the act focuses too heavily on traditional cybersecurity threats and may not be agile enough to keep up with rapidly evolving cyber threats.[161] As a result, the Commission had recently proposed an amendment (18 April 2023) to the Act as this will allow the management of security services for proper incorporation of European certification schemes in the future.[162]

In addition to the above points, the Web has made a tremendous universal network that has produced billions of dollars yearly for the worldwide economy.[163] As of now, a large portion of the financial, business, social, social and legislative exercises and cooperations of countries, at all levels, including government and administrative foundations, are done on the Internet.[164] Crucial and sensitive structures and frameworks either form part of the internet or are controlled oversaw and taken advantage of through this space, and a large portion of the sensitive and vital data is moved to this space. Most media exercises are moved to this space, most financial trades are finished through this space and a critical extent of residents' time and exercises are spent communicating here.[165] Therefore, as a result, Governments and regulatory bodies regularly take a proactive approach to ensure cybersecurity by working with the private sector to identify emerging threats and implement effective solutions.

[160] 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). Retrieved from http://data.europa.eu/eli/reg/2019/881/oj 15 April 2023.

[161] Ferreira, A., & Sandner, P. (2021). Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. *Computer Law & Security Review*, *43*, 105632.

[162] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[163] Judge, M. A., Manzoor, A., Maple, C., Rodrigues, J. J., & ul Islam, S. (2021). Price-based demand response for household load management with interval uncertainty. *Energy Reports*, *7*, 8493-8504.

[164] *Ibid.*

[165] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

CONCLUSION

The main objective of the research was to establish a comparative analysis of cybersecurity legislation of connected products with digital elements for small and medium-sized businesses in the UK and the EU. The significance of the findings explained that due to the increasing cyber-security threats and data attacks, all businesses must have strong cybersecurity systems that can help in protecting small and mid-sized businesses entity and highlighting the risk points which can help in making the system safe. If there are any kind of failures in the security the business can have financial losses and the business can have serious issues such as the loss of entity. The cybersecurity market has the potential to grow in the coming years because of its importance in protecting data. Cybersecurity has become an essential aspect of businesses and organisations worldwide. To minimize cybercrime and ensure data protection, different countries have established and proposed laws to mention such as the Data Protection Act (2018) the EU CRA etc, while organisations like ENISA and ESCO have been set up to tackle the problem. The European Cybersecurity Skill Framework and the increase in cyber insurance also emphasize the importance of cybersecurity. However, there is still a need for continuous improvement and implementation of effective cybersecurity measures to mitigate the risks of cybercrime.

The UK and the EU share several similarities in their legal frameworks for cybersecurity, including their focus on data security, their establishment of acts and laws to protect sensitive information, their investment in cybersecurity, and their formation of organisations to reduce cybercrime activities. Both have recognized the importance of addressing cybersecurity issues and have taken steps to prevent data theft, modification, and leakage. This is reflected in the significant investments made to improve cybersecurity systems and reduce cyber-attacks. While the UK PSTI Bill and the EU CRA share a common goal of improving cybersecurity, they differ in their scope and approach. The CRA focuses on all sectors and sets out some mandatory requirements that are to be fulfilled by the producer, manufacturer or distributor for a time of five years. This specific section is probably going to turn into a test for some organizations and become a challenge for many companies, as ensuring the security is up to date should likewise be made accessible for those devices that can only supposedly create an online connection, whereas the PSTI Bill targets mainly two sectors – the product security and the telecommunications industry and therefore sets minimum-security requirements. Both regulations provide penalties for non-compliance, highlighting the importance of companies and organisations taking cybersecurity seriously to maintain consumer trust and ensure safety and security. The UK's PSTI legal framework and the EU CRA share a significant overlap in their legal perspectives on cybersecurity. Both prioritize the safety and security of citizens' data and digital infrastructure, with a particular focus on ICT products and services. Businesses operating across both regions must ensure compliance with relevant laws and regulations to meet the required cybersecurity standards. Cybersecurity is a crucial aspect of businesses and organisations worldwide, and the UK and the EU have taken significant steps to address the issue. Continuous improvement and implementation of effective cybersecurity measures are necessary to mitigate the risks of cybercrime.

To conclude, the UK and the EU governments have recognised the critical need to address cybersecurity legislation, particularly concerning connected products with digital elements for SMEs. The UK PSTI Bill and the EU CRA both aim to improve cybersecurity measures and reduce the risk of cyberattacks. However, there are differences in scope and mandatory compliance across member states. While the support of a more secure open internet is crucial for promoting communication, innovation, and growth, protecting individual rights and freedoms in the digital age is also essential. Digital security has become a major concern, especially for SMEs, due to the increasing use of technology in business operations and the constant evolution of cybercriminal tactics. SMEs are particularly vulnerable to data theft and the associated financial, reputational, and legal consequences. The UK government report highlights the pressing need for increased awareness and investment in cybersecurity measures for SMEs. Therefore, this thesis aims to explore the impact of cybersecurity legislation on connected products for SMEs in the UK and the EU, examine the effectiveness of current cybersecurity measures, and identify opportunities for improvement. This study contributes to addressing the identified problem and highlighting its significance in protecting the interests of individuals, businesses, and organisations. The findings of this thesis can inform policymakers, businesses, and stakeholders in enhancing cybersecurity measures and mitigating the risk of cyberattacks for SMEs in the UK and the EU.

The increase in cyber insurance and the European Cybersecurity Skill Framework also highlights the importance of cybersecurity. However, there is still a need for continuous improvement and implementation of effective cybersecurity measures to mitigate the risks of cybercrime. The similarities between the legislations state that the legislation systems of both the UK and the EU share several features in terms of their focus on ensuring data security, establishing acts and laws to protect sensitive information, investing in cybersecurity, and forming organisations to reduce cybercrime activities. Both countries have recognised the importance of addressing cybersecurity issues and have taken steps to prevent data theft, modification and leakage.

Further Research

A potential research recommendation could be to evaluate the differences in scope and mandatory compliance across member states, as well as the impact of cybersecurity legislation on connected products for SMEs in both regions. The research could also explore the challenges faced by SMEs in implementing effective cybersecurity measures and identify opportunities for improvement. The study could utilise a mixed-methods approach, combining quantitative data analysis with qualitative interviews or surveys of SME owners and cybersecurity experts. In addition to that, the research implications of this thesis are significant for policymakers, businesses, and stakeholders in the UK and the EU. First, the findings of this study can inform policymakers on the effectiveness of current cybersecurity legislation and identify areas for improvement. The study can also highlight the need for increased investment in cybersecurity measures, particularly for SMEs, which are most vulnerable to cyberattacks. Secondly, the study can provide insights for businesses in developing and implementing robust cybersecurity systems that meet the required standards. The research can help businesses understand the potential risks of cyberattacks and the associated financial, reputational, and legal consequences. This understanding can motivate businesses to invest in cybersecurity measures to protect their confidential information and ensure business continuity. Thirdly, the study can help stakeholders in the cybersecurity industry identify opportunities for improvement and innovation. Stakeholders can use this information to develop new products and services that meet the changing needs of businesses and organisations in the digital age.

As the threat of cyberattacks continues to increase, the findings from this study can inform policymakers, businesses, and stakeholders in enhancing cybersecurity measures and mitigating the risk of cyberattacks. Similarly, contributes to addressing the critical need for cybersecurity and adequate legislation for SMEs in the UK and the EU. Future research can build on the findings of this thesis by exploring other cybersecurity measures (prevention of malware, network security, etc) and identifying best practices for SMEs in the UK and the EU. For example, investigate the value of employee training programs, software updates, and incident response plans in reducing the risk of cyberattacks. Moreover, there is a need to investigate the impact of emerging technologies such as artificial intelligence and the Internet of Things on cybersecurity and data protection. Finally, future research can examine the impact of cybersecurity legislation on businesses and organisations in other regions or how third-world countries are embracing cybersecurity development and compare their approaches to the UK and EU.

LIST OF REFERENCES

Scientific Books

1. DeNardis, L. (2020). *The Internet in everything*. Yale University Press.

2. Dillon, R., Lothian, P., Grewal, S., & Pereira, D. (2021). Cyber security: evolving threats in an ever-changing world. In *Digital Transformation in a Post-COVID World* (pp. 129-154). CRC Press.

3. European Commission. (2020). Cybersecurity Our Digital Anchor. A European Perspective.

4. Holloway, D. (2018). Iii Discursive Constructions Of The Internet Of Toys Lelia Green Donell Holloway. *Digitising Early Childhood*, 226.

5. Kertysova, K., Frinking, E., van den Dool, K., Maričić, A., & Bhattacharyya, K. (2018). Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks-Study. European Economic and Social Committee: Bruxelles, Belgium.

6. Ollino, Alice. *Due diligence obligations in international law*. Cambridge University Press, 2022.

Scientific Articles

7. Akanle, O., Ademuson, A. O., & Shittu, O. S. (2020). Scope and limitation of the study in social research. *Contemporary Issues in Social Research*, 105-114.

8. Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1-5). IEEE.

9. Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. *Sensors*, *21*(20), 6901.

10. Alsharari, N. M., & Al-Shboul, M. (2019). Evaluating qualitative research in management accounting using the criteria of "convincingness". *Pacific Accounting Review*.

11. Amarasinghe, S. L., Su, S., Dong, X., Zappia, L., Ritchie, M. E., & Gouil, Q. (2020). Opportunities and challenges in long-read sequencing data analysis. *Genome biology*, *21*(1), 1-16.

12. Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580.

13. Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410.

14. Badran, H. (2019, June). IoT security and consumer trust. In *Proceedings of the 20th Annual International Conference on Digital Government Research* (pp. 133-140).

15. Barrett, Catherine. "Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection?." *SciTech Lawyer* 15, no. 3 (2019): 24-29.

16. Benson, V., Furnell, S., Masi, D., & Muller, T. (2021). Regulation, Policy, and Cybersecurity.

17. Bhatia, N. L., Shukla, V. K., Punhani, R., & Dubey, S. K. (2021, June). Growing Aspects of Cyber Security in E-Commerce. In *2021 International Conference on Communication Information and Computing Technology (ICCICT)* (pp. 1-6). IEEE.

18. Bocayuva, M. (2021). Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic. *WMU Journal of Maritime Affairs*, *20*(2), 173-192.

19. Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU the example of the financial sector: a legal perspective. *German Law Journal*, *21*(6), 1149-1179.

20. Car, P., & De Luca, S. (2022). EU cyber-resilience act.

21. Castilho Salgues, I. A. (2020). *The EU Cybersecurity Framework: An evaluation of the Framework's approach in tackling cyberattacks* (Master's thesis).

22. Chander, Anupam, Meaza Abraham, Sandeep Chandy, Yuan Fang, Dayoung Park, and Isabel Yu. "Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation." *Policy Research Working Paper* 9594 (2021).

23. Chandna, V., & Tiwari, P. (2023). Cybersecurity and the new firm: Surviving online threats. *Journal of Business Strategy*, *44*(1), 3-12.

24. Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. *International Cybersecurity Law Review*, 1-18.

25. Child, J. (2021). Computer Misuse Act 1990: CLRNN1: Comparative Report.

26. Codagnone, C., Liva, G., & de las Heras Ballell, T. R. (2022). Identification and assessment of existing and draft EU legislation in the digital field. *Study for the Special Committee on Artificial Intelligence in a Digital Age (AIDA). Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg*.

27. De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. International Journal of Law and Information Technology, 30(1), 68-87.

28. Deepak, G. C., Ladas, A., Sambo, Y. A., Pervaiz, H., Politis, C., & Imran, M. A. (2019). An overview of post-disaster emergency communication systems in the future networks. *IEEE Wireless Communications*, *26*(6), 132-139.

29. Dutton, W. H., Creese, S., Esteve-Gonzalez, P., Goldsmith, M., & Weisser Harris, C. (2022). Next steps for the EU: building on the Paris Call and EU cybersecurity strategy. *Available at SSRN 4052728*.

30. Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Fatima, Z. (2020). Cyber attacks in the era of covid-19 and possible solution domains.

31. Farelo, N. M. D. A. (2023). Design of a Security Toolbox: A Framework To Mitigate The Risks of Cyberspace (Doctoral dissertation).

32. Ferreira, A., & Sandner, P. (2021). EU searches for regulatory answers to crypto assets and their place in the financial markets infrastructure. Computer Law & Security Review, 43, 105632.

33. Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity regulation in the European Union: the digital, the critical and fundamental rights. *The ethics of cybersecurity*, 97-115.

34. Harkins, D. (2020). Data Protection & Freedom of Information Policy. *Policy*.

35. Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204.

36. Howell, C. J. Cybercrime Investigation-Readings. Murdoch University Electronic Journal of Law, 8(2), 2-42.

37. Jelinek, T. (2023). Technology Silos of Today or the End of Global Innovation. In *The Digital Sovereignty Trap: Avoiding the Return of Silos and a Divided World* (pp. 19-33). Singapore: Springer Nature Singapore.

38. Jeyaraj, A., & Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity: A text analytics approach. *Journal of Organizational Computing and Electronic Commerce*, *30*(4), 361-380.

39. Judge, M. A., Manzoor, A., Maple, C., Rodrigues, J. J., & ul Islam, S. (2021). Price-based demand response for household load management with interval uncertainty. Energy Reports, 7, 8493-8504.

40. Junjie, M., & Yingxin, M. (2022). The Discussions of Positivism and Interpretivism. *Online Submission*, *4*(1), 10-14.

41. Kempen, A. (2019). Cybercrime knows no borders. *Servamus Community-based Safety and Security Magazine*, *112*(8), 27-31.

42. Kertysova, K., Frinking, E., van den Dool, K., Maričić, A., & Bhattacharyya, K. (2018). Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks-Study. *European Economic and Social Committee:* Bruxelles, Belgium.

43. Khan, M. J. (2023). Securing network infrastructure with cyber security. *World Journal of Advanced Research and Reviews*, *17*(2), 803-813.

44. Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O. T. S., & Vergara, R. G. (2022). A systematic literature review on cybercrime legislation. *F1000Research*, *11*(971), 971.

45. Krishna, B., Krishnan, S., & Sebastian, M. P. (2022). Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: an institutional trust theory perspective. *Information Systems Frontiers*, 1-29.

46. Krüger, P. S., & Brauchle, J. P. (2021). The European Union, cybersecurity, and the financial sector: A primer.

47. Kuzmanovic, A. (2019). Net neutrality: unexpected solution to blockchain scaling. *Communications of the ACM*, *62*(5), 50-55.

48. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

49. Le Nguyen, C., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries:'Law on the books' vs 'law in action. *Computer Law & Security Review*, *40*, 105521.

50. Lemon, L. L., & Hayes, J. (2020). Enhancing trustworthiness of qualitative findings: Using Leximancer for qualitative data analysis triangulation. *The Qualitative Report*, *25*(3), 604-614.

51. Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., ... & He, B. (2021). A survey on federated learning systems: vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*.

52. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

53. Lindqvist, J. (2018). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *International Journal of Law and information technology*, 26(1), 45-63.

54. Ludvigsen, K. R., & Nagaraja, S. (2022). The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity Resilience Act. *arXiv preprint arXiv:2205.13196*.

55. Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors*, *19*(1), 19.

56. Mangku, D. G. S., Yuliartini, N. P. R., Suastika, I. N., & Wirawan, I. G. M. A. S. (2021). The Personal Data Protection of Internet Users in Indonesia. *Journal of Southwest Jiaotong University*, *56*(1).

57. Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, 35(6), 105336.

58. McKeown, J. (2023). A data-driven analysis of UK cyber defence. arXiv preprint arXiv:2303.07313.

59. Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: an architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems, 15(4), 565-584.

60. Mihai, I. C., Ciuchi, C., & Petrică, G. (2023). The Latest Challenges in the Cybersecurity Field. In Regulating Cyber Technologies: Privacy vs Security (pp. 1-18).

61. Mutalib, M. M. A., Zainol, Z., & Halip, M. H. M. (2021, December). Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework. In *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)* (Vol. 6, pp. 1-6). IEEE.

62. Nikolopoulou, Antonia. "The Directive on the Security of Networks and information systems (NIS Directive) from a practical view." (2019).

63. O'REILLY, P. A. T. R. I. C. K., & Rigopoulos, K. (2022). Fiscal Year 2021 Cybersecurity & Privacy Annual Report. *NIST SPECIAL PUBLICATION*, *800*, 220.

64. Onwujekwe, G., Thomas, M., & Osei-Bryson, K. M. (2019, April). Using robust data governance to mitigate the impact of cybercrime. In *Proceedings of the 2019 3rd International Conference on Information System and Data Mining* (pp. 70-79).

65. Osula, A. M. (2022). Building Cyber Resilience: The Defensive Shield for the EU. In *Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives* (pp. 179-196). Cham: Springer International Publishing.

66. Oxford Analytica. (2022). EU cybersecurity rules to raise pressure on IoT firms. Emerald Expert Briefings, (oxan-db).

67. Paul, P. K. (2023). Wireless Sensor Network (WSN) Vis-à-Vis Internet of Things (IoT): Foundation and Emergence. In *Computational Intelligence for Wireless Sensor Networks* (pp. 1-16). Chapman and Hall/CRC.

68. Ponsard, C., Grandclaudon, J., & Dallons, G. (2018). Towards a Cyber Security Label for SME: A European Perspective-. ICISSP, 4, 426-431.

69. Quinn, H. (2023). The Information Commissioner's Response to the Government's AI White Paper.

70. Ramadhan, N., & Rose, U. (2022). Adapting ISO/IEC 27001 Information Security Management Standard to SMEs.

71. Rixhon, P. (2022). New Media Business Models to Emerge from the Internet of Value. *Enabling the Internet of Value: How Blockchain Connects Global Businesses*, 87-102.

72. Ruggiano, N., & Perry, T. E. (2019). Conducting secondary analysis of qualitative data: Should we, can we, and how?. *Qualitative Social Work*, *18*(1), 81-97.

73. Saleem, M. (2019, June). Brexit impact on cyber security of United Kingdom. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-6). IEEE.

74. Salvi, A., Spagnoletti, P., & Noori, N. S. (2022). Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, *112*, 102507.

75. Scauso, M. S. (2020). Interpretivism: Definitions, trends, and emerging paths. In *Oxford Research Encyclopedia of International Studies*.

76. Schmitz-Berndt, S., & Chiara, P. G. (2022). One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International Cybersecurity Law Review*, *3*(2), 289-311.

77. Scott, H. S. (2021). The EU's Digital Operational Resilience Act: Cloud Services & Financial Companies. *Available at SSRN 3904113*.

78. Sharma, R. Legislation Related to Cyber Crimes in the United Kingdom.

79. Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). Cybersecurity: Legal And Organizational Support In Leading Countries, Nato And Eu Standards. *Journal of Security & Sustainability Issues*, *9*(3).

80. Shukla, M., Johnson, S. D., & Jones, P. (2019, June). Does the NIS implementation strategy effectively address cyber security risks in the UK? In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-11). IEEE.

81. Singh, H. P., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: a case of Saudi Arabia. *Beijing L. Rev.*, *11*, 637.

82. Spencer, A., & Patel, S. (2019). Applying the data protection act 2018 and general data protection regulation principles in healthcare settings. *Nursing Management*, *26*(1).

83. Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, *92*, 178-188.

84. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

85. Sullivan, J., & Nurse, J. R. (2021). Cyber security incentives and the role of cyber insurance. *RUSI Emerging Insights Paper*.

86. Tam, Tracy, Asha Rao, and Joanne Hall. "The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses." *Computers & Security* 109 (2021): 102385.

87. Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J. J. (2019). The United Kingdom's emerging Internet of Things (IoT) policy landscape. *Tanczer, LM, Brass, I., Elsden, M., Carr, M., & Blackstock, J.(2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance*, 37-56.

88. Turianskyi, Y. (2020). Africa and Europe: cyber governance lessons.

89. Vagena, E., & Ntellis, P. (2020). Cybersecurity legislation: Latest evolutions in the EU and their implementation in the Greek legal system. EU Internet Law in the Digital Era: Regulation and Enforcement, 239-259.

90. Van den Abeele, E. (2021). Towards a new paradigm in open strategic autonomy? ETUI Research Paper-Working Paper.

91. Vilić, V. (2019). Phishing and pharming as forms of identity theft and identity abuse. Balkan Social Science Review, 13(13), 43-57.

92. Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. Colum. Bus. L. Rev., 494.

93. Walters, R., & Novak, M. (2021). Cyber security. In *Cyber security, artificial intelligence, data protection & the law* (pp. 21-37). Singapore: Springer Singapore.

94. Wan, Y., Fu, L. H., Li, C., Lin, J., & Huang, P. (2021). Conquering the hypoxia limitation for photodynamic therapy. Advanced Materials, 33(48), 2103978.

95. Wilkinson, S. (2022). UK data protection and digital information bill explained. Journal of Data Protection & Privacy, 5(3), 242-253.

96. Wilson, M., McDonald, S., Button, D., & McGarry, K. (2022). It Won’t Happen to Me: Surveying SME Attitudes to Cyber-security. Journal of Computer Information Systems, 1-13.

97. Wilson, S. (2020). The pandemic, the acceleration of digital transformation and the impact on cyber security. *Computer Fraud & Security*, *2020*(12), 13-15.

98. Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. SN Computer Science, 3(2), 127.

99. Yang, Qiang, Yang Liu, Tianjian Chen, and Yongxin Tong. "Federated machine learning: Concept and applications." ACM Transactions on Intelligent Systems and Technology (TIST) 10, no. 2 (2019): 1-19.

100. Yoo, J. (2022). Recent Trends in UN Cybersecurity Governance and South Korea-EU Cooperation. In Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives (pp. 235-250). Cham: Springer International Publishing.

101. Zachariadis, M., & Ozcan, P. (2017). The API economy and digital transformation in financial services: The case of open banking.

102. Zgraggen, R. R. (2019, June). Cyber Security Supervision in the insurance sector: smart contracts and chosen issues. In 2019 international conference on cyber security and protection of digital services (cyber security) (pp. 1-4). IEEE.

103. Zou, B., Choobchian, P., & Rozenberg, J. (2020). Cyber Resilience of Autonomous Mobility Systems: Cyber Attacks and Resilience-Enhancing Strategies. World Bank Policy Research Working Paper, (9135).

Legislations

104. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680, Accessed on 09 May 2023.

105. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from http://data.europa.eu/eli/dir/2016/1148/oj, Accessed on 15 April 2023

106. Legislation.gov.uk. 1990. "Computer Misuse Act 1990." Legislation.gov.uk. 1990. https://www.legislation.gov.uk/ukpga/1990/18/contents

107. Parliament, U. K. Product Security and Telecommunications Infrastructure (PSTI) Bill (2022). Retrieved from https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted, Accessed on 19 April 2023.

108. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj, Accessed on 09 May 2023.

109. 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). Retrieved from https://eur-lex.europa.eu/eli/reg/2019/881/oj Accessed on 15 April 2023.

110. Regulation of the European Parliament and the Council on horizontal cybersecurity requirements for products with Digital elements and amending Regulation (EU) 2019/1020. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454 Accessed on 03 May 2023.

Other Sources

111. European Commission, (15 September 2022). Shaping Europe#s Digital Future: Cyber Resilience Act. *Policy and legislation.* Retrieved from https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act, Accessed on 15 April 2023.

112. Gareth, C. (2019). Guilty of hacking in the UK? Worry not. Retrieved from https://www.theregister.com/2019/05/29/computer_misuse_act_prosecutions_analysis/, Accessed on 03 April 2023.

113. IEC Innovation Report 2019. https://webstore.iec.ch/publication/65943

114. "Investigatory Powers Act." n.d. GOV.UK. https://www.gov.uk/government/collections/investigatory-powers-bill#:~:text=On%20Tuesday%2029%20November%202016

115. Molly.K. (19 April 2023). EU launches Cyber Solidarity Act to respond to large-scale attacks – EURACTIV.com.

116. EU Policy Updates - EU Policy Update – February 2023 - CENTR

117. https://bluexp.netapp.com/blog/data-compliance-regulations-hipaa-gdpr-and-pci-dss

118. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

119. https://ecs-org.eu/european-cybersecurity-and-resilience-what-challenges-to-create-a-common-framework/

120. https://edps.europa.eu/data-protection/our-work/publications/legislation/regulation-eu-20181725_en#:~:text=Regulation%20(EU)%202018%2F1725%20of%20the%20European%20Parliament%20and,EC)%20No%2045%2F2001%20and

121. https://eucrim.eu/news/edps-provides-opinion-on-cybersecurity-directive/#:~:text=The%20current%20EU%20Network%20and,functioning%20of%20the%20internal%20market.

122. https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/#:~:text=The%20UK%20eIDAS%20Regulations%20set,certificate%20services%20for%20website%20authentication.

123. https://kpmg.com/de/en/home/insights/2023/02/cyber-security-in-the-eu-nis-2-directive-increases-security-levels.html#:~:text=NIS%2D2%20directive%20raises%20common,of%20all%20EU%20member%20states.&text=The%20European%20Union%20is%20strengthening,force%20on%2016%20January%202023.

124. https://products.cooley.com/2023/01/05/medical-devices-and-ivds-fall-outside-the-scope-of-the-proposed-cra-but-for-how-long/

125. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

126. https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets

127. https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/telecoms-security-proposal-for-new-regulations-and-code-of-practice

128. https://www.ifsecglobal.com/cyber-security/product-security-and-telecommunications-infrastructure-psti-act-2022-what-does-it-cover/

129. https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted

130. https://www.lexology.com/library/detail.aspx?g=d29fa051-c36f-4fb0-9ec8-be2c09711242

131. https://www.taylorwessing.com/en/insights-and-events/insights/2023/01/uk-introduces-new-rules-on-the-security-of-connected

products#:~:text=The%20PSTI%20Act%20gives%20the,them%20available%20in%20the%20UK

132. https://www.wareable.com/health-and-wellbeing/wearable-tech-and-regulation-5678

APPENDICES

Appendix 1.

1.1 The top countries with the maximum cybercrime density.

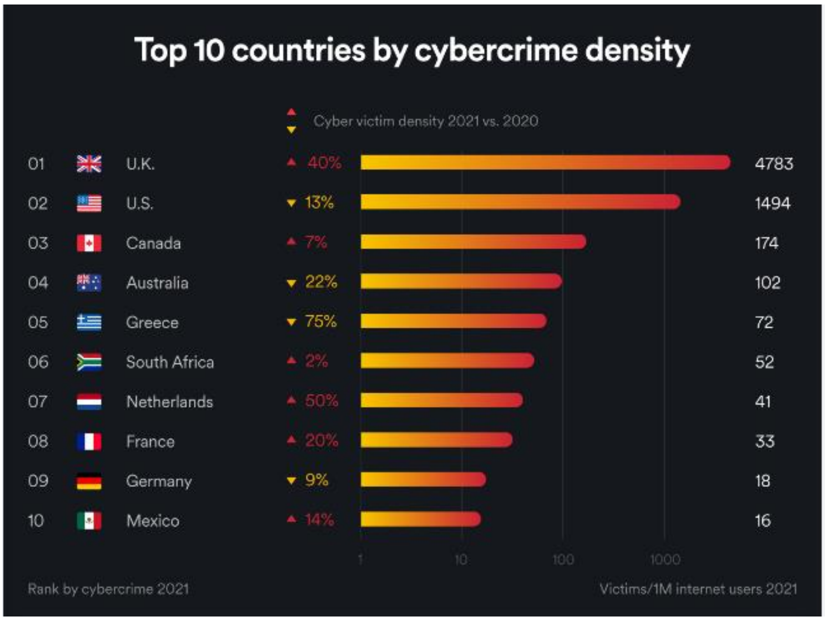


Figure 7. Top countries with maximum cybercrime density.

Source: Cook, S., et.al. (2023).

Appendix 2. Non-exclusive licence

Non-exclusive licence for reproduction and for granting public access to the graduation thesis [i]

I Mosebolatan Grace Adu,

1. Give Tallinn University of Technology permission (non-exclusive licence) to use free of charge my creation – **Support of A Secure Open Internet: A Comparative Analysis of the UK and EU Cybersecurity Legislation on Connected Products with Digital Element for SMEs**,
   Supervised by- Dr Agnes Kasper:

   1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;
   1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third person's intellectual property rights or the rights arising from the personal data protection act and other legislation.

[i] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*