

# **Ensuring Cybersecurity Compliance: Assessing SME Awareness and Preparedness for the Cyber Resilience Act**

**Christoph Szedlak<sup>1</sup>, Holger Reinemann<sup>1</sup>, Sophia Hatzelmann<sup>2</sup>**

<sup>1</sup>Competence Center of Digitalization  
Koblenz University of Applied Science  
Koblenz 56075, Germany  
ahc GmbH  
70376 Stuttgart, Germany

## **Abstract**

The rapid advancement of digital technology has ushered in the "fourth industrial revolution," characterized by the seamless integration of technologies across physical, digital, and biological domains. Within this context, the European Union's Cyber Resilience Act (CRA) aims to establish uniform cybersecurity standards for all digital products, thereby enhancing the overall cyber resilience of the EU market. This study explores the level of awareness and preparedness among small and medium-sized enterprises (SMEs) regarding the CRA. A quantitative survey was conducted, gathering 673 responses from 416 SMEs, 160 large companies, and 91 very large enterprises. The findings reveal significant disparities in CRA awareness and readiness, with only 12.3% of SMEs being aware of the CRA compared to 83.5% of very large enterprises. SMEs reported substantial challenges including a shortage of skilled labor, lack of a comprehensive cybersecurity strategy, and uncertainties about the CRA's specifics. In contrast, very large enterprises focused on timeline pressures and achieving compliance. These results underscore the urgent need for targeted support and resources to address the specific needs of each enterprise group. Furthermore, the study highlights the necessity for SMEs to adopt a proactive stance in monitoring and understanding regulatory changes to mitigate risks associated with late compliance. The research contributes valuable insights into the effectiveness of current communication and implementation strategies surrounding the CRA and suggests potential areas for improvement to achieve the overarching goal of widespread cyber resilience. Future studies should validate these findings and explore the impact of enhanced regulatory pressure and diversified communication channels on improving CRA awareness and compliance among SMEs.

## **Keywords**

Cyber Resilience, Cyber Security, SME, Cyber Resilience Act

## **1. Introduction**

The swift evolution of digital technology has catalyzed the onset of what is widely recognized as the "fourth industrial revolution," which is characterized by the seamless integration of technologies that blur the boundaries between the physical, digital, and biological spheres (Schwab 2016). A critical component of this revolution is the Internet of Things (IoT), a framework that underpins the modern information society by facilitating the interconnection of both tangible and virtual entities through established and evolving technological platforms (Carr & Lesniewska 2020). Currently, the proliferation of IoT devices exceeds the global human population, and forecasts suggest that by 2025, approximately 30.9 billion devices will be operational worldwide, with over 4.3 billion within the European Union alone (Analytics 2020). This inevitably results in a larger attack surface due to the numerous devices that are, for the most part, insufficiently protected.

In an era where digital transformation is reshaping business landscapes, Small and Medium-sized Enterprises (SMEs), in particular, find themselves increasingly vulnerable to cyber threats (Hayes & Bodhan 2013). These organizations, often operating with limited resources and expertise, are prime targets for cyber-attacks, making the need for robust cybersecurity measures more critical than ever (McLaurin 2021). Against this backdrop, the Cyber Resilience Act (CRA) has emerged as a pivotal piece of legislation aimed at bolstering the cybersecurity framework across the European Union (European Commission 2022). However, the effectiveness of such regulatory measures largely depends on the awareness and preparedness of the entities they aim to protect. This article delves into the findings of a quantitative survey conducted to assess the level of awareness and understanding of the Cyber Resilience Act among SMEs.

## **1.1 Objectives**

The primary objective of this study is to ascertain the level of awareness and preparedness among SMEs regarding the CRA recently enacted by the European Union. This research aims to identify how well-informed SMEs are about the CRA, evaluate their readiness to comply with its requirements, and understand the cybersecurity strategies currently in place. Additionally, the study seeks to uncover the major challenges SMEs face in enhancing their cybersecurity measures in line with CRA guidelines. By exploring these areas, the research will contribute valuable insights into the effectiveness of current communication and implementation strategies surrounding the CRA, and suggest potential areas for improvement.

## **2. Fundamentals and Impacts of the CRA on SME**

### **2.1 The Key Aspects of the CRA**

The CRA, detailed in more than seventy Recitals and almost 60 Articles including 6 Annexes, seeks to establish a cohesive cybersecurity framework. This framework mandates that products with digital components maintain security throughout the supply chain and their entire lifecycle, while also empowering users to prioritize cybersecurity in their selection and use of these products (European Commission 2022).

The subject matter of the CRA encompasses four primary elements:

1. **Regulatory Guidelines for Market Entry:** Establishing rules for the introduction of products with digital elements into the market to ensure their cybersecurity.
2. **Design and Production Standards:** Defining essential requirements for the design, development, and production of digital products, alongside outlining the cybersecurity obligations of economic operators associated with these products.
3. **Vulnerability Management:** Specifying essential requirements for manufacturers' vulnerability handling processes to ensure the cybersecurity of digital products throughout their lifecycle, as well as the related obligations for economic operators.
4. **Market Surveillance and Enforcement:** Setting forth rules for the monitoring and enforcement of the aforementioned regulations and requirements.

Through these comprehensive measures, the CRA aims to enhance the cybersecurity posture of digital products, fostering a more resilient and secure digital ecosystem. In the context of the impending CRA, Member States are mandated to establish rules on penalties for infringements by economic operators, ensuring these are effective, proportionate, and dissuasive. Severe non-compliance with the essential cybersecurity requirements and specific obligations could lead to administrative fines of up to 15 million EUR or up to 2.5% of an entity's total worldwide annual turnover for the previous financial year, whichever is higher. Economic operators have a 24-month window to align their operations with the CRA before these regulations become mandatory, underscoring the urgency for immediate action to meet these comprehensive cybersecurity standards (European Commission 2022).

### **2.2 Affected Companies by the CRA**

The CRA encompasses a broad spectrum of stakeholders within the digital product ecosystem, mandating stringent cybersecurity measures across all stages of product development and distribution. Key stakeholders include software and hardware manufacturers, importers, distributors, and end-users, each bearing distinct responsibilities to ensure compliance (CEC 2019). Manufacturers are required to integrate cybersecurity features from the design phase through to production and post-market surveillance. Importers and distributors must verify that the products they handle meet CRA standards, acting as critical intermediaries in maintaining market integrity. Market surveillance authorities, along

with accreditation and notifying bodies, are tasked with monitoring compliance and enforcing regulations to prevent non-compliant products from reaching consumers (European Commission 2022).

The CRA's reach extends across various sectors, notably information and communications technology (ICT), automotive, medical, and financial industries. ICT products and services must adhere to existing certification frameworks under the Cybersecurity Act (EU/2019/881). In the automotive sector, vehicles must comply with cybersecurity management regulations. Medical products are required to safeguard sensitive health data, while financial products are governed by directives like the NIS 2.0 and the upcoming Digital Operational Resilience Act (DORA). According to a market analysis conducted by Eurostat, over 23,000 hardware manufacturers in the EU are impacted, despite these sectors already being subject to partial regulatory oversight. Remarkably, 97.13% of these entities are classified as small and medium-sized enterprises (SMEs). Furthermore, only a modest proportion, about 4%, are medium-sized companies, employing up to 250 individuals. This distribution pattern is similarly observed within the software sector, cumulating to more than 200,000 SMEs in the ICT sector (Eurostat 2019). Additionally, a significant number of manufacturers incorporate affected components in their products, which are procured as parts and integrated into final assemblies. This comprehensive regulatory approach ensures that cybersecurity risks are managed throughout the entire lifecycle of digital products, enhancing the cyber resilience of products in the EU market. The CRA thereby mandates a unified framework to protect against evolving cyber threats, ensuring that all stakeholders, from manufacturers to end-users, maintain robust cybersecurity standards.

### **2.3 The Concept of Cyber Resilience**

The evolution of technology has expanded the scope of information security into the broader realm of cybersecurity, which not only encompasses the protection of the confidentiality, integrity, and availability (CIA triad) of information but also extends to safeguarding other assets (Solms & Niekerk, 2013). Traditionally, the focus in this field has largely been on protection and detection, but recent trends have shifted towards incorporating a more comprehensive incident response (Sharikov 2019). This shift has given rise to the concept of cyber resilience, which integrates human elements and strategic processes into cybersecurity, marking a departure from purely technological solutions. Cyber resilience is viewed by some as a subset of cybersecurity focusing on response mechanisms (Cybenko 2016; Aoyama, et al., 2015), while others perceive it as an all-encompassing approach that includes anticipating, detecting, withstanding, recovering from, and evolving after cyber threats. Furthermore, strategic and human processes are included (Linkov, et al. 2013; Sharkov 2016).

The distinct nature of cyber resilience lies in its objectives which prioritize maintaining business continuity over mere protection of IT systems, embracing a safe-to-fail mindset rather than a fail-safe one, and advocating for a holistic approach over an isolated focus on individual organizations (Björk et al. 2015). Cyber resilience thus represents a multidimensional and multidisciplinary endeavor (Nys 2016), necessitating diverse areas of knowledge and a proactive strategy in its operationalization, especially for SMEs. These smaller entities often adopt a reactive stance towards cybersecurity (Schneier 2014), which may leave them less protected than anticipated (Hollnagel et al. 2006), underscoring the importance of a systematic approach to implementing cyber resilience.

### **2.4 Cyber Security Situation for SMEs**

SMEs play a pivotal role in global economies but are increasingly targeted by cyber threats due to perceived vulnerabilities and inadequate cyber defenses (Hayes & Bodhan, 2013). Despite their economic significance, SMEs often lack the financial and human resources to implement robust cyber security measures, leaving them exposed to a spectrum of cyber risks. McLaurin (2021) highlights that these entities often attract less experienced cyber criminals due to their relatively weaker security measures, stemming from a mistaken belief in their existing safeguards. This vulnerability also is compounded by the reliance on outdated security frameworks (Carias et al. 2021) and a limited understanding of cyber risks among SME management (Saban et al. 2021; Löffler et al. 2021). In addition, current literature overlooked SMEs specific needs (Ikuro & Zeng. 2022).

A 2020 Verizon report underscores that cyber attacks are indiscriminate, affecting organizations of all sizes and sectors (Widup, et al. 2020). However, research indicates that SMEs are less likely to invest in advanced cyber security technologies or employ dedicated cyber security personnel compared to larger organizations, which can allocate more resources towards mitigating cyber threats (Huelsman & Peasley 2016; Fielder et al. 2016). Consequently, SMEs suffer disproportionately from cyber-attacks, with impacts ranging from financial losses to significant disruptions in operations (Damiano 2019). Moreover, the rapid pace of technological change and the evolving nature of cyber threats further challenge SMEs' ability to stay protected. Particularly at risk are mobile and other Internet of Things (IoT)

devices in the SME environment, which are often the weakest links allowing attackers entry into networks (Polkowski & Dysarz 2017; Heikkila, et al. 2016).

To address these challenges, it is crucial for SMEs to embrace a holistic approach to cyber security, integrating both technological and human factors into their cyber defense strategies, adapting the idea of cyber resilience (Deutscher, et al. 2017; Goldman, et al. 2016). The adoption of comprehensive cyber security frameworks, such as the NIST Cyber Security Framework (National-Institute-of-Standards-and-Technology 2023), the international standard ISO 27001 providing best-practice specifications (Information Technology 2005) or the CRA provided structured guidance and improve resilience against cyber threats. Additionally, fostering a culture of cyber awareness and continuous learning can empower SMEs to better anticipate, detect, and respond to cyber incidents, thereby enhancing their overall cyber resilience.

### **3. Methods**

#### **3.1 Survey Development**

To address the research question concerning the level of awareness of the CRA among SMEs, a quantitative online questionnaire was developed. The questionnaire was meticulously crafted to capture both the breadth and depth of CRA awareness, preparedness, and the cybersecurity strategies currently employed by SMEs. The survey consisted of a series of structured questions designed to assess:

- The degree of awareness of the CRA among the respondents.
- The readiness of the respondents to comply with the CRA regulations.
- The challenges faced by respondents in implementing robust cybersecurity practices.
- Sources from which respondents received information regarding the CRA.

The questions were primarily close-ended, allowing for quantitative analysis, with multiple-choice, Likert-scale, and yes/no formats to simplify the responses and facilitate statistical analysis. Based on the definition of products with digital elements, eligible participants were pre-sorted. After an initial inquiry about the contents and effects of the CRA, participants were provided with a brief summary of the CRA in the form of a video (3.2 minutes) to ensure a uniform understanding of the CRA for the subsequent questions. Finally, the main hurdles and the effects on their own company and its preparedness were inquired about again.

#### **3.2 Survey Distribution and Data Collection**

The distribution of the questionnaire was strategically executed using automated, personalized emails targeted at companies potentially affected by the CRA. This process was initiated with comprehensive lists from three regional chambers of commerce as the foundational data source. In an effort to enhance the efficiency of this outreach and minimize the rate of irrelevant responses, a preliminary sorting of these companies was conducted. For example, only legal entities were considered. Sole proprietors, etc., were excluded from the survey. Ultimately, this meticulous approach enabled the identification of complete contact details for 5,283 individuals, thereby ensuring a focused and effective sampling for the study. The data collection phase extended over a six-week period, from March 10th to April 20<sup>th</sup> 2024. This duration was deliberately selected to afford ample opportunity for a substantial cohort of respondents to contribute. This methodical approach was vital to ensure the comprehensiveness and reliability of the data gathered. Ultimately, 673 complete responses were counted, resulting in a response rate of 12.75%.

#### **3.3 Demographics**

The 673 responses are distributed among 416 SMEs, of which two-thirds are manufacturers and one-third are providers. Among the large companies, defined as those with 250 to 1,000 employees and a revenue of €50 Mio to €500 Mio, there are 160 respondents. The very large enterprises, defined as those with more than 1,000 employees and a revenue exceeding €500 million, account for 91 respondents. A self-assessment of cybersecurity and resilience was conducted using a 7-point Likert scale, ranging from "not at all" to "completely prepared." On average, micro enterprises reported a score of 3.4, while very large enterprises reported a score of 5.2. Only responses indicating a connection to products with digital elements were considered.

Table I. Demographics of participating enterprises

	Micro	Small	Medium	Large	Very Large
Manufacturers	61	101	110	86	56
Providers	13	40	91	74	41
Total	74	141	201	160	97
Level of Cyber Security	3.4	2.6	3.1	4.3	5.2

### 3.4 Ethical Considerations

Prior to participation, all respondents were informed about the purpose of the survey and the anonymous nature of the data collection process. Consent was obtained from all participants, with assurances that all responses would be treated with the strictest confidentiality and that data would be reported only in aggregate form. No personally identifiable information was collected in the survey, aligning with general data protection regulations and ethical standards of research.

## 5. Results and Discussion

### 5.1 Awareness of the CRA

The findings reveal a significant disparity in CRA awareness between SMEs and large enterprises. Specifically, 83.5% of companies with more than 1,000 employees reported being aware of the CRA and its requirements, compared to only 12.3% of SMEs. Within the SME group, no significant differences were observed among micro, small, and medium-sized enterprises ( $\chi^2(2, N = 416) = 3.26, p = .196$ ). A difference between providers and manufacturers could also not be observed. Figure 1 shows the awareness divided by company size in absolute numbers.

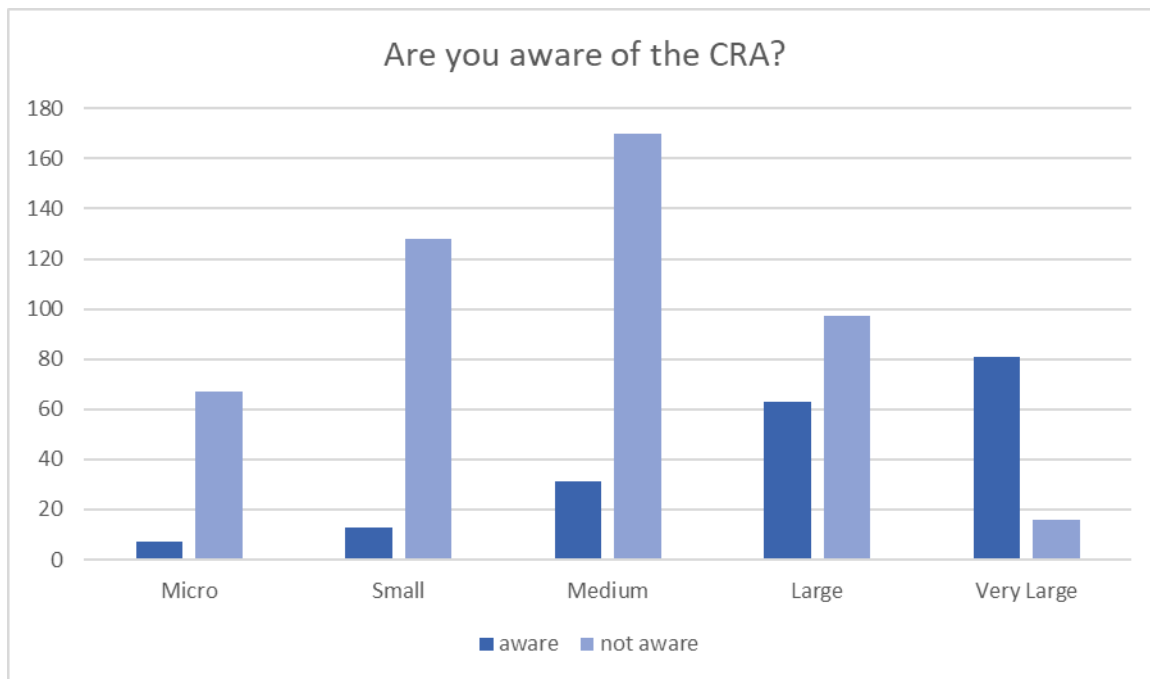


Figure 1. Awareness of CRA depends on company size. Absolute values (n=673)

Notably, only 19% of the 416 SMEs surveyed indicated that they actively and regularly stay informed about regulatory requirements such as the CRA. Most SMEs that are aware of the CRA became informed by chance or through external sources. In contrast, 61% of large companies and 93% of very large companies reported regularly staying informed about such regulations.. Considering that the CRA was introduced in 2019 and its implementation has been almost certain since 2022, it is perplexing that the proportion of companies actively seeking information is significantly higher than the proportion that is actually aware of the CRA. This discrepancy is even more pronounced when taking into account those who became informed by chance. This raises important questions about the effectiveness of

communication and outreach efforts regarding regulatory changes. It is essential to further sensitize SMEs to obtain information early and proactively to be prepared for upcoming regulations, so the time-related risk of implementation difficulties shrinks.

Overall, the findings underscore the persistent gap in Cyber Resilience Awareness among SMEs. The underlying causes of this gap are currently under investigation, revealing a pattern of resignation and overwhelm among SMEs, largely attributed to inadequate resources and a deficiency in robust frameworks and guidelines. This presents a critical leverage point; enhancing regulatory pressure could significantly bolster Cyber Resilience efforts. By addressing these deficiencies, we can promote a proactive and sustainable approach to increasing protective measures across the sector.

### 5.2 Perceived Readiness to Comply with the CRA

The majority of SMEs, following a brief introduction to the CRA, expressed an inability to independently comply with the CRA requirements within the stipulated timeframe. This perceived inadequacy was predominantly attributed to their insufficient preparation for incorporating a "design by security" process in product development, fulfilling the extensive reporting mandates, integrating an appropriate risk management framework, and implementing comprehensive vulnerability management protocols as illustrated in Figure 2. The latter presents a significant challenge, particularly for small and medium-sized enterprises, which they believe they cannot overcome without external support, leading to a high demand for resources. Overall, all companies feel they are not yet well-prepared.

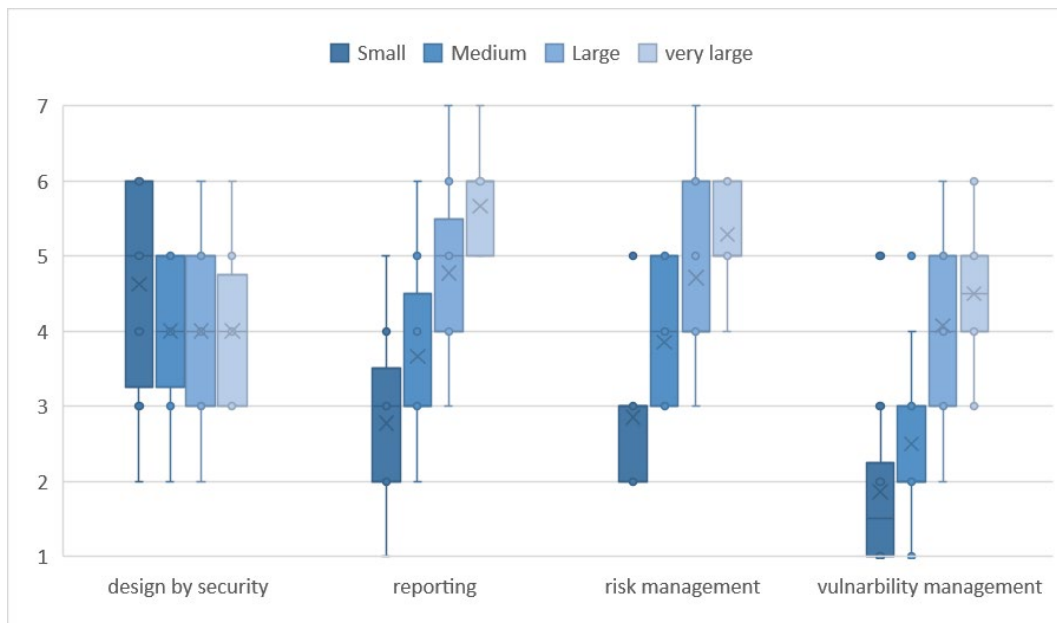


Figure 2. Self-assessment of companies regarding their preparedness to comply with important CRA components (n=673)

Only 60% of SMEs that had already engaged with the CRA could assess whether and to what extent their own company would be affected by it. The others were provided with a summary of the relevant section from the proposal. Only 1 in 5 stated that they could classify their own products into the specified categories based on this information. Accordingly, it is particularly important to provide clarity on which products are affected by the CRA. This should go beyond the existing examples to make the entire topic more accessible and comprehensible.

### 5.3 Main Challenges Faced by SMEs

SMEs are the backbone of all developed economies and the digital transformation of these companies is crucial for economic growth (OECD 2021). However, there is a significant digitization gap in SMEs, largely due to resource limitations. Financial investment poses a major challenge, as SMEs often struggle to secure the necessary funds due to limited access to capital markets and uncertain costs associated with digital transformation projects. Additionally, the perception of digital technologies in SMEs is limited; many SMEs, especially family-managed ones, are risk-averse and miss out on growth and innovation opportunities. The availability of skilled workers also significantly

impacts SME digitization efforts, with a notable positive relationship between digital activities and the presence of academically qualified employees. These challenges are critical as SMEs prepare for the imminent enforcement of the CRA, making it essential to address these barriers to enhance their cyber resilience and secure their future in a digital economy (Szedlak & Reinemann 2023).

Figure 3 provides a clear depiction of the diverse challenges encountered by small, medium, and very large enterprises in the context of CRA implementation. For SMEs, the shortage of skilled labor emerges as a predominant issue, as indicated by the substantial proportion of respondents identifying this concern. This issue is further compounded by significant uncertainty regarding the specifics of the CRA, presenting a substantial barrier for these companies. The absence of a comprehensive cyber security strategy adds another layer of difficulty, hindering SMEs' ability to ensure compliance with the CRA's mandates.

Medium-sized enterprises similarly report notable challenges with skilled labor shortages and CRA-specific uncertainties. However, the absence of a cyber security strategy is less pronounced compared to SMEs, suggesting some level of preparedness in this domain. Despite this, compliance and timeline pressures remain significant concerns for medium-sized companies, indicating areas where further support may be necessary. In contrast, very large enterprises primarily highlight challenges related to the timeline and the complexities of achieving compliance. This group appears to possess a relatively robust understanding of the CRA and a more developed cyber security strategy. Nonetheless, the practical aspects of compliance within the prescribed timelines continue to present significant hurdles.

The data underscore a critical insight: while SMEs struggle with more generalized challenges such as resource limitations and strategic deficiencies, very large enterprises focus more on the practicalities of compliance within the given timelines. This distinction emphasizes the necessity for tailored support and resources that address the specific needs of each group, facilitating a smoother transition to CRA compliance across the entire spectrum of enterprise sizes.

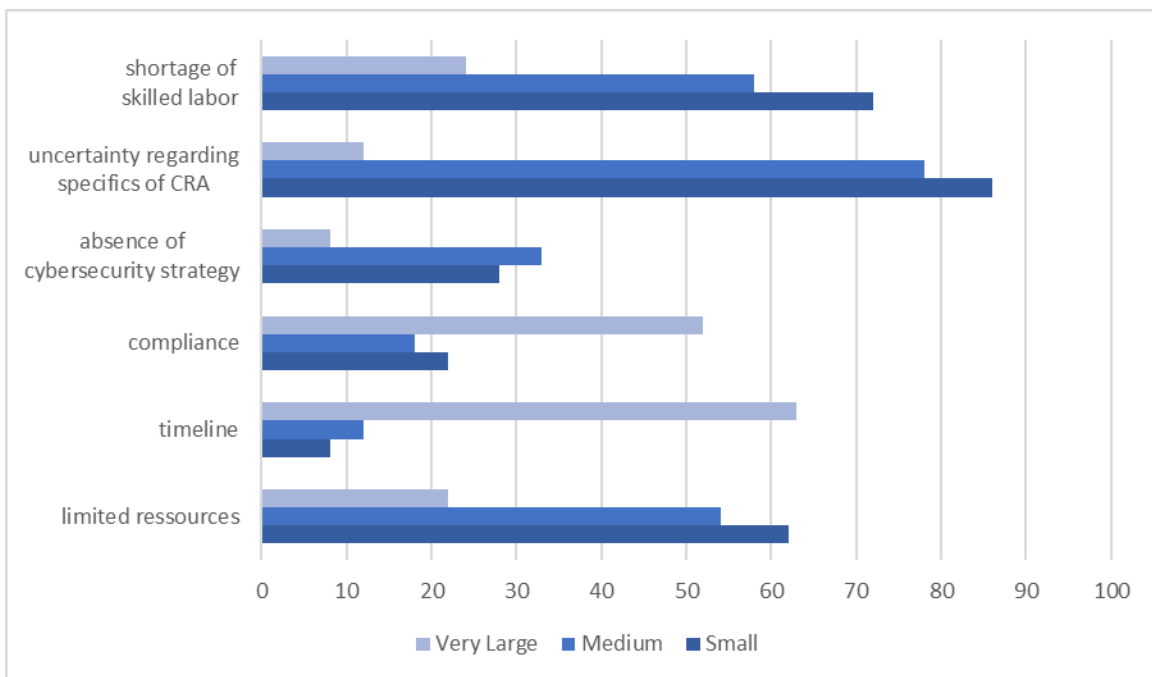


Figure 3. Comparison of main challenges faced by SMEs and very large companies

#### 5.4 Source of Information

The principal findings reveal a noteworthy deficiency in awareness regarding the CRA among SMEs. A mere fraction of surveyed SMEs demonstrated familiarity with CRA. Knowledge predominantly derives from professional

associations (28%), business news websites (19%), industrial conferences (9%), and trade journals (17%). A survey of preferred information sources indicates a majority favor business news (64%), trade journals (51%), television (31%), and social media (27%) as primary channels. Strikingly, almost none of the participants cited government websites as a preferred source (<1%). This observation highlights a critical need for government agencies to reevaluate outreach strategies. To enhance CRA awareness and knowledge among SMEs, these agencies should consider utilizing more widely frequented and accessible platforms. Multichannel communication can keep enterprises informed throughout the finalization phase.

Given that many are concerned about the time horizon and the need for high investments to comply with CRA regulations, adopting earlier information strategies for SMEs is necessary. A significant portion of informed companies sources information from professional associations and industrial conferences. However, these channels attract only a minority, contributing to the existing information gap. Note the different sample sizes (n) in the figure.

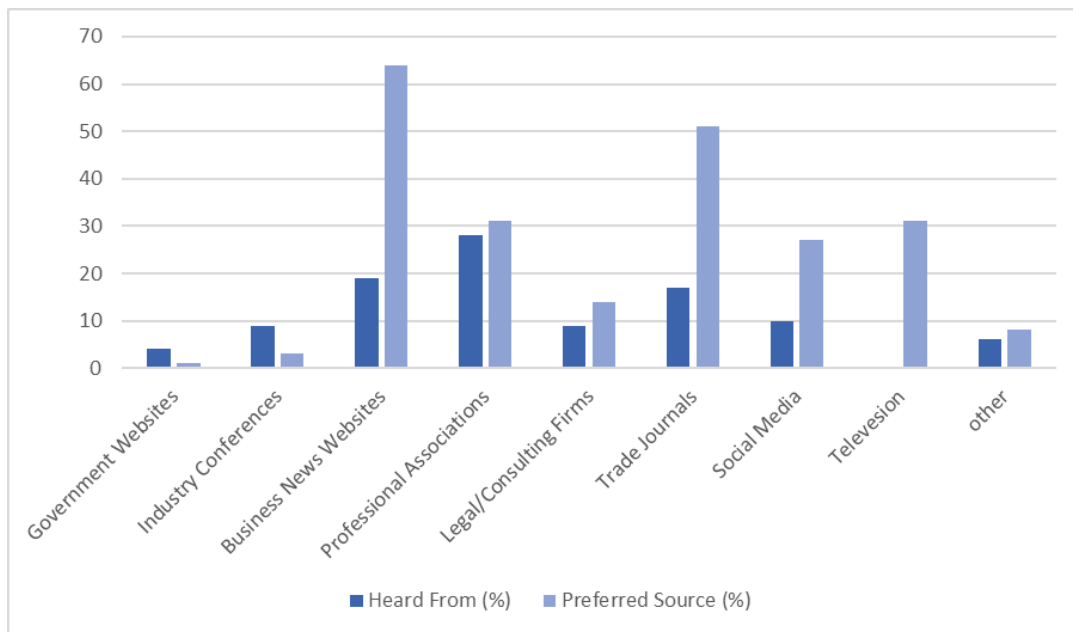


Figure 4. Information Sources for SMEs Aware of CRA (n=51 ) and Preferred Information Sources for All SMEs (n=416 )

## 6. Conclusions

Although the CRA has far-reaching implications for companies with products containing digital elements, which can lead to severe consequences after a transition period if not complied with, the majority of SMEs do not feel capable of implementing the legal requirements within the given time and do not consider these regulations to be reasonable with regard to cyber risk prevention. Furthermore, a significant information gap is evident among SMEs, which predominantly believe that the responsibility for adhering to regulatory requirements such as the CRA lies with the authorities, and do not proactively seek out information in advance. Typically, these companies only begin actively gathering information after the regulations have come into effect, which conflicts with the challenge of having a short response time. This reactive approach undermines their ability to adequately prepare for compliance, that might lead to rushed efforts to meet legal obligations. Consequently, there is a pressing need for SMEs to adopt a more proactive stance in monitoring and understanding regulatory changes to mitigate the risks associated with late compliance.

Accordingly, there should be not only a general awareness raised about the topic but particularly about Cyber Resilience. The discrepancy between actively seeking information about impending regulatory changes and actual awareness can likely be partly attributed to the preferred communication media, such as business news websites and trade journals. Reporting has predominantly occurred in specialized media, which a large proportion of SMEs do not consult due to their general lack of awareness about Cyber Resilience.

To bridge this gap, it is crucial to diversify the channels through which information about regulatory changes and Cyber Resilience is disseminated. This could include leveraging more accessible and frequently used platforms by SMEs, such as social media, industry newsletters, and regional business networks. Additionally, targeted campaigns and educational initiatives could help enhance SMEs' understanding of the importance of proactive information-seeking and the critical nature of Cyber Resilience in safeguarding their operations against emerging threats. The objective must be to establish a uniform baseline to address the information deficit prevalent among SMEs. This would provide a solid foundation that, with the assistance of skilled professionals, would facilitate implementation. Such an approach would enable a shift in focus towards the practical attainment of compliance rather than being mired in structural issues. Only through this strategy can the timely implementation of the CRA be realized, ultimately achieving the overarching goal of widespread cyber resilience. These assumptions need to be validated in future studies.

However, this study focuses exclusively on German companies, despite the necessity for a comparative European perspective on the Cyber Resilience Act (CRA). The structure of SMEs in Germany differs significantly from that in other European countries, which could influence the generalizability of the findings. Although the results underline the urgent need to address the situation in SMEs, it is essential to extend this research to other European countries to gain a comprehensive understanding of the CRA's implications across the continent. Given the imminent enforcement of the CRA, it is crucial to further investigate and prepare for its impact on SMEs throughout Europe. Furthermore, due to the participation rate, a distortion of the results cannot be ruled out, as a high number of unreported cases regarding awareness and preparedness is likely to prevail.

## References

- Aoyama, T. et al., Studying resilient cyber incident management from large-scale cyber security training. *Proceedings 10th Asian Control Conference (ASCC)*, pp. 1-4,2 015.
- Björk, F., Henkel, M., Stirna, J. & Zdravkovic, J., Cyber resilience–fundamentals for a definition. *Adv. Intell. Syst. Comput.* Band 353, pp. 3-4,2015.
- Carias, J. F., Arrizabalaga, S., Labaka, L. & Hernantes, J., Cyber Resilience Self-Assessment Too for SMEs. *IEEE Access*, Band 9, pp. 80741-80762,2021.
- Carr, M. & Lesniewska, F., *Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance*, s.l.: International Relations,2020.
- CEC, C. o. t. E. C. C. o. t., 2019., *Second Interim Study Report N 2019-0024 supporting the impact assessment*, Brussels: Eurostat.
- Cybenko, G., 2016., Quantifying and measuring cyber resiliency. *Proceedings SPIE*, Band 9825.
- Damiano, M., 2019. *IPRE Announces Launch of VIPRE Endpoint Security-Cloud Edition*, s.l.: Business Wire.
- Deutscher, S., Bohmayr, W. & Asen, A., 2017. *Building a cyberresilient organization*. Boston, MA: s.n.
- EC, E. C., 2022. *Annex I - Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) 2019/102*, Brussels: European Union.
- European Commission, 2022., *Proposal for a Regulation of the european parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending regulation*, Brussels: European Commission.
- Eurostat, 2019. *SBS\_NA\_SCA\_R2 supporting impact study*, Brussels: Eurostat.
- Fielder, A. et al., Decision support approaches for cyber security investment. *Decision Support Systems*, Band 86, pp. 13-23, 2016.
- Goldman, H., McQuaid, R. & Picciotto, J., 2016., Cyber resilience for mission assurance. *Proceedings IEEE International Conference on Technological Homeland Security*, pp. 236-241.
- Hayes, J. & Bodhan, A., 2013. Cyber security: Small firms under fire. *Engineering Technology*, 8(6), pp. 80-83.
- Heikkila, M., Rattya, A., Pieska, S. & Jamsa, J., Security Challenges in small- and medium-sized manufacturing enterprises. *Proceedings International Symposium on Small-Scale Intelligent Manufacturing Systems*, pp. 25-30,2016.
- Hollnagel, E., Woods, D. & Leveson, N., 2006. *Resilience Engineering: Concepts and Precepts*. Hampshire: Ashgate Pub Co.
- Huelsman, T. & Peasley, S., 2016., *Cyber risk in advanced manufacturing*. Richmond: s.n.
- Ikuero, F. & Zeng, W., *Improving Cybersecurity Incidents Reporting in Nigeria: Micro and Small Enterprises Perspectives*, s.l, 2022.: <https://doi.org/10.4314/njt.v41i3.10>.

- Information Technology, S. T., 2005. , *Code of Practice for Information Technology Security Techniques*, Geneva, Switzerland: International Organization Standardization.
- IoT Analytics, 2020., *Internet of Things (IoT) and Non-IoT Active Device Connections Worldwide from 2010 to 2025*. [Online]  
Available at: <<https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/>> [Zugriff am June 2024].
- KfW. KfW-Digitalisierungsbericht, Frankfurt, 2024
- Linkov, I. et al., Resilience metrics for cyber systems. *Environmental Systems Decisions*, 33(4), pp. 471-476,2013.
- Löffler, E., Schneider, B., Zanwar, T. & Asprien, P. M., SecEscape 2.0—A Virtual Escape Room To Raise Cybersecurity Awareness. *International Journal of Serious Games*, 8(1), pp. 59-70,2021.
- McLaurin, T., 2021. *A study on the efficacy of small business cybersecurity controls*, Marymount: ProQuest Dissertations Publishing.
- National Institute-of-Standards-and-Technology, 2023. *Evolution of teh framework*. [Online]  
Available at: <https://www.nist.gov/cyberframework/evolution>  
[Zugriff am Jun3 2024].
- Nys, J., 2016. How to steer cyber security with only one KPI: The cyber risk resilience. *Proc. RSA Conference* , pp. 1-42.
- OECD, The Digital Transformation of SME, OECD Studies on SMEs and Entrepreneurship, Paris: OECD Publishing, 2021
- Polkowski, Z. & Dysarz, J., IT security management in small and medium enterprises. *Sci. Bull. - Econ. Sci.*, 16(3), pp. 134-148,2017.
- Saban, K., Rau, S. & Wood., C., 2021. SME executives' perceptions and the information security preparedness model. *Information and Computer Security*, 29(2), pp. 263-282.
- Schneier, B., The future of incident response. *IEEE Secur. Privacy*, 12(5), pp. 96-97,2014.
- Schwab, K., 2016. *The fourth industrial revolution*, Geneva: s.n.
- Sharikov, P., Evolution of American cyber security policies. *World Economic Int. Relations*, 63(10), pp. 51-58,2019.
- Sharkov, G., From cybersecurity to collaborative resiliency. *Proc. ACM Workshop Automated Decis. Making Act. Cyber Defense Co-Located CCS (SafeConfig)*, pp. 3-9,2016.
- Solms, R. v. & Niekerk, J. c., From information security to cyber security. *Computer Security*, Band 38, pp. 97-102,2013.
- Szedlak, Ch. & Reinemann, H., Digital Technology Use among Small and Medium Sized Enterprises, Proceedings of the IEOM International Conference on Smart Mobility and Vehicle Electrification Detroit, Michigan, USA, October 10-12, 2023
- Widup, S. et al. Verizon: Data breach investigations report 2020. *Comput. Fraud. Secur.*, Band 6, p. 4,2020.

## **Biographies**

**Christoph Szedlak** is the Director of the Competence Center for Digitalization for SMEs.

**Holger Reinemann** is Professor for SME Management at the University of Applied Science Koblenz.

**Sophia Hatzelmann** is the Managing Director of ahc GmbH and a Industry 4.0 Scout for the state of Baden-Württemberg.