How to overcome Human error in IT-Security - The employment of Marketing and Sales in the Cyber Security Awareness Training Sector.

Nils Hünemeier
University of Bochum
Benedikt Hirschfelder
University of Cape Town
Sascha Alavi
University of Bochum

Cite as:
Hünemeier Nils, Hirschfelder Benedikt, Alavi Sascha (2021), How to overcome Human error in IT-Security - The employment of Marketing and Sales in the Cyber Security Awareness Training Sector.. *Proceedings of the European Marketing Academy*, 50th, (94560)

Paper from the 50th Annual EMAC Conference, Madrid, May 25-28, 2021

How to overcome Human error in IT-Security - The employment of Marketing and Sales in the Cyber Security Awareness Training Sector.

Abstract:

One of the best defenses against cybercrime is to train the users on cyber security awareness as 50% of successful attacks could be avoided, if users where more aware of today's cyber threats. Unfortunately, only 40% of German companies train their employees regarding cybercrime. Therefore, the marketing of Cyber Defense Awareness (CDA) Trainings is extremely important to secure company data and the wellbeing of the European economy in the long run. The aim of this paper is to explore possible marketing channels to further sell and employ CDA Trainings. In order to combine the fields Cyber Security and Marketing, this interdisciplinary study developed a framework providing insights into customer interest while searching for CDA Trainings. The results illustrate the ability to influence potential customers and provide a basis for future research.

Keywords: *Cyber Defense Awareness Training, Referral Marketing, Search Engine Marketing*

Track: *Innovation Management & New Product Development*

1. Introduction

1.1. Problem statement

In 2019, the "Bundesverband Informationswirtschaft, Telekommunikation und neue Medien" (Federal Association for Information Technology, Telecommunications and New Media) confirmed in a survey, that 88% of German companies have been victims of data theft, industrial espionage and/or sabotage in the past two years. If the analogue and digital attacks are added together, the German economy suffers a total annual loss of 102.9 billion euros (Berg & Niemeier, 2019). Cyber-attacks are considered the greatest risk to the existence of companies in today's cyber environment. Half of all attacks are caused by human error because untrained employees are an ideal gateway into company systems (Grüter, 2019).

The work environment is rapidly evolving and constantly changing, and users within must constantly adapt to it. Securing these networks is of critical importance to ensure that corporate data is safe, there is no data theft, espionage, or sabotage. One of the most important defenses in the field of IT cyber security is the human capital of companies. However, to be able to use this potential, it is essential to train employees. For this reason, training courses in the area of Cyber Defense Awareness (CDA) have been offered more frequently in recent years. But only approximately 40% of German companies use this tool to make their employees an active line of defense against cybercrime.

The fact that about 60% of companies do not train their employees has devastating consequences. In 2016, a successful cyberattack on a company took place every 40 seconds. This number of successful cyberattacks has more than doubled in recent years. It is assumed that the frequency of successful attacks will go up to one attack every 11 seconds in 2021 (Morgan, 2019). The German economy suffers a total annual loss of 102.9 billion euros due to cyber criminality (Berg and Niemeier, 2019). Therefore, Cyber Defense Awareness Trainings offer enormous potential for the active commercialization of these programs, especially in the B2B environment.

The technological progress in the past 20 years offers marketing practitioners a wide array of marketing channels to communicate with their audience. It is more important than ever, to choose the right communication channels and to find a good balance between them (Scharf *et al.*, 2015). According to Kluge and Gronau (2018) intentional forgetting of, for example defective private cyber security behavior, has a major impact on implementing organizational learning. However, as Cyber Defense Awareness Trainings are a niche product in the training market, there are no scientific studies concerning the marketing of CDA Trainings. Hence, the focus of this paper is on the effect of the individual marketing channels on the interest and therefore, the willingness to buy and employ Cyber Defense Awareness Trainings in B2B markets.

2. What is Cyber Security Awareness

Cyber security awareness refers to how much end users know about the cyber security threats their networks face and the risks they introduce (Kim, 2017). End users are considered the weakest link and the primary vulnerability within a network (Kemper, 2019). Therefore, it is of utmost importance, that companies educate employees on current threats and how to avoid them. Kumaraguru and Sheng (2010) analyzed the effect of Cyber Defense Awareness Trainings on companies and confirmed the effectiveness of cyber defense trainings in several studies. However, it was proven that the effects of Cyber Defense Awareness Trainings fade away after about 4-6 months. Accordingly, it is extremely important to train every user of a company network on a regular basis (Alnajim & Munro, 2009; Canova et al., 2015; Mayr & Pinzger, 2016; Reinheimer et al., 2020).

For this reason, this study analyses which marketing communication channels are most meaningful to influence new and existing customers into buying and employing Cyber Defense Awareness Trainings.

3. Framework Development

A total of 19 different marketing channels were analyzed. After all communication channels were examined, they were grouped together. All communication channels were considered and assigned to one of the two categories: "*Customer Pull*" and "*Company Push*". Should the initial information contact result from a customer request it is considered a "*Customer Pull*". All communication channels that can be brought to the customers attention by an active push are assigned to the "*Company Push*" category (Brocato, 2010). In a second step the communication channels are further divided to make the questionnaire more accessible for the public and to reduce the number of necessary questions. The following seven main marketing channels were identified and categorized.

Push Category				Pull Category		
Social Media	“Traditional” Online Advertisement	“Traditional” Offline Advertisement	Referral	Search Engines	On Demand Information Material	On Demand Personal Information
Social Media Posts Social Media Ads	Direct Mail Printed Ads Magazines	Google Ads In-App Ads Banner Ads Video Ads Newsletter	Customer Referral	Organic Searches	Case Studies Blog Articles Whitepaper Informative Websites Infographics Free Trials	Webinars Personal Appointments Product Presentations Trade Fairs Events

Table 1: Categorization of marketing channels

The basic assumption of the work was that all seven categories of communication channels have a positive influence on the customer's interest and thus purchase decision.

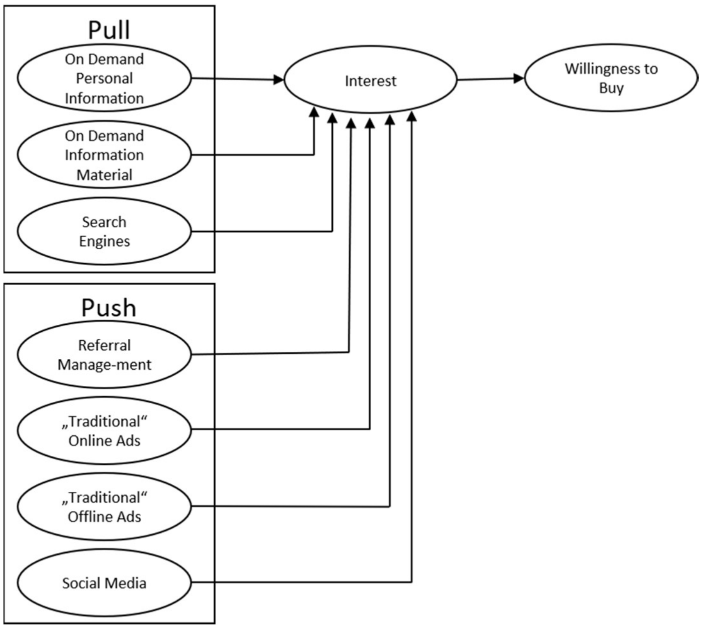


Figure 1: Structural model

4. Methodology

In order to generate the scientific data basis for the research, a quantitative research approach in the form of a survey was chosen. A comprehensive questionnaire was designed for this purpose (Hussy et al., 2013, S. 75). The questionnaire was designed deductively based on different theories.

4.1. Sample size and data collection

According to Hoyle (1995) and Wong (2013), a good starting point for path modelling is a sample size of 100 to 200. Since the nature of research is exploratory, a non-probability convenience sampling was adopted (Malhotra & Birks, 2006). In total 242 questionnaires were completed. After a pre-evaluation, eliminating incomplete and not suitable questionnaires, 228 questionnaires were used for the data analysis. The research was geographically limited to Germany and Belgium. The target group were participants between the age of 18 and 65.

4.2. Measurement

Due to the fact that academic literature and research on Cyber Defense Awareness Training Marketing is relatively rare, the questionnaire was partly based on the following sources:

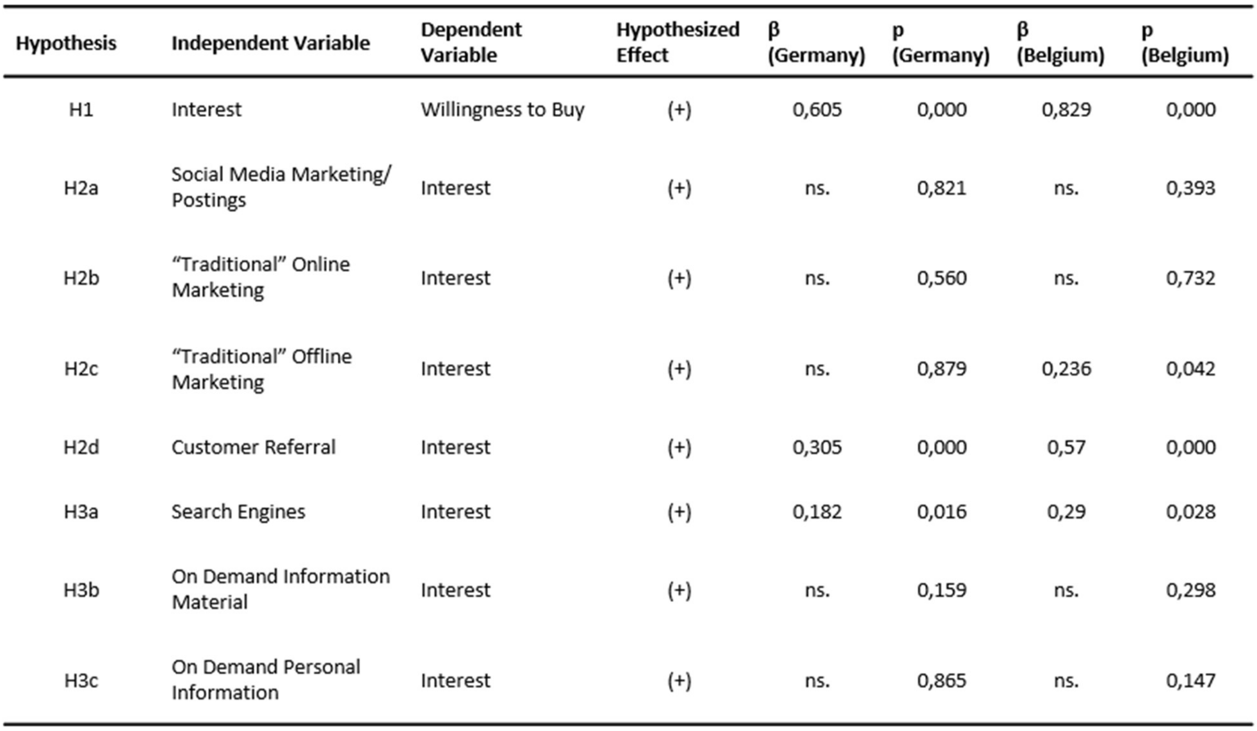
Bock et al. (2006), Marez et al. (2007), Chanchary & Chiasson (2015), Eleonora (2015), Schivinski et al. (2016). The independent constructs as well as the dependent construct were operationalized and measured with 5-point Likert-type scale.

4.3. Data analysis

To test the hypothesized model, a partial least squares structural equation modelling approach was used. As a consequence thereof, the researchers made use of the software package SmartPLS.

5. Results

With regard to the measurement model, internal consistency reliability (Cronbach's alpha, composite reliability), validity (composite reliability, AVE) and discriminant validity (HTMT) were verified. With the exception of the AVE for the construct Online Ads, which deviated from the norm (0,204 in Germany, 0,81 in Belgium) all constructs fulfilled the requirements. Since the measurement scale is still in development, the deviation was excepted.



Hypothesis	Independent Variable	Dependent Variable	Hypothesized Effect	β (Germany)	p (Germany)	β (Belgium)	p (Belgium)
H1	Interest	Willingness to Buy	(+)	0,605	0,000	0,829	0,000
H2a	Social Media Marketing/ Postings	Interest	(+)	ns.	0,821	ns.	0,393
H2b	"Traditional" Online Marketing	Interest	(+)	ns.	0,560	ns.	0,732
H2c	"Traditional" Offline Marketing	Interest	(+)	ns.	0,879	0,236	0,042
H2d	Customer Referral	Interest	(+)	0,305	0,000	0,57	0,000
H3a	Search Engines	Interest	(+)	0,182	0,016	0,29	0,028
H3b	On Demand Information Material	Interest	(+)	ns.	0,159	ns.	0,298
H3c	On Demand Personal Information	Interest	(+)	ns.	0,865	ns.	0,147

Table 2: Structural Results

Regarding the structural model, it can be inferred from Table 2, that three hypotheses were supported. Accordingly, H1 indicates, that the interest in Awareness Trainings is directly influencing the willingness to buy them. Furthermore, it can be inferred that Customer Referrals and Search Engines have a positive influence on the interest in CDA Trainings. The relationships between the other marketing channels and interest are not significant, indicating that they do not have a significant impact on consumer interest.

6. Implications:

6.1. Future research and limitations

Since CDA Trainings in media-based form are relatively new, current marketing is based more on trial and error than on scientific evidence. Hence, there are critical knowledge-gaps regarding the effectiveness of communication channels. For this reason, this paper was written to lay a foundation for further research. This paper benefited from already existing marketing knowledge and created a tailored concept to explore marketing in a business-to-business IT Security Training market. However, since the work, by dividing the different marketing channels into subgroups, can only give a broad overview of the topic it is necessary to continue the research. Online offers are becoming more and more interesting, especially due to the changes on the job market caused by Covid 19 (Shalini Shah *et al.*, 2020).

Since this paper primarily provides an overview of all marketing channels, it is important for a deeper understanding that the individual marketing channels are further illuminated. Using this study as groundwork, it would be appropriate to look at the channels individually rather than in groups for future research.

6.2. Marketing and sales

It was confirmed that search engine and referral management have a positive influence on the interest of the customers in CDA Trainings, and therefore the purchase decision. Hence, it is advisable for CDAT service provider to further improve SEO as well as Customer Referral Programs, to reach and influence new customers and existing customers. However, it should be mentioned that these results do not mean that marketing should be limited to these two communication channels only, because marketing is a holistic process (Sheth & Sisodia, 2006) and can also indirectly affect the individual [e.g. "mere exposure effect"] (Harrison, 1977).

7. Conclusion

The main finding of this thesis is that search engine marketing and referral management have a direct influence on the interest of customers in Cyber Defense Awareness Training and that this direct effect indirectly influences the purchase decision. These influences could be verified not only for Germany, but also for its neighboring country Belgium.

The main purpose of this research was to gain a scientifically sound insight into the marketing of Cyber Defense Awareness Trainings in a B2B environment. The resulting framework and the hypotheses confirmed by this research provide new insights on the theoretical and management side. In summary, this paper reduces the gap between the academic knowledge about marketing in IT-B2B markets and the practical application of marketing channels and provides a basis for future research.

8. References

Alnajim, A., & Munro, M. (2009). An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection. *2009 Sixth International Conference on Information Technology: New Generations*, 405–410. https://doi.org/10.1109/ITNG.2009.109

Berg, A., & Niemeier, M. (2019). *Angriffsziel deutsche Wirtschaft: Mehr als 100 Milliarden Euro Schaden pro Jahr | Bitkom e.V.* Bundesverband Informationswirtschaft, Telekommunikation und neue Medien. https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr

Bock, G.-W., Kankanhalli, A., & Sharma, S. (2006). Are Norms Enough? The Role of Collaborative Norms in Promoting Organizational Knowledge Seeking. *EJIS*, *15*, 357–367. https://doi.org/10.1057/palgrave.ejis.3000630

Brocato, D. (2010). Push and Pull Marketing Strategies. In J. Sheth & N. Malhotra (Hrsg.), *Wiley International Encyclopedia of Marketing* (S. wiem01053). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781444316568.wiem01053

Canova, G., Volkamer, M., Bergmann, C., & Reinheimer, B. (2015). NoPhish App Evaluation: Lab and Retention Study. *Proceedings 2015 Workshop on Usable Security*. Workshop on Usable Security, San Diego, CA. https://doi.org/10.14722/usec.2015.23009

Chanchary, F., & Chiasson, S. (2015). User Perceptions of Sharing, Advertising, and Tracking. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 53–67. https://www.usenix.org/conference/soups2015/proceedings/presentation/chanchary

Eleonora, P. (2015). *Successful Technological Integration for Competitive Advantage in Retail Settings*. IGI Global.

Grüter, P. (2019). *Pitchdeck: Cyber Defense Awareness Trainings—Schützen Sie Ihr Unternehmen vor Social Engineering, Phishing und Ransomware.* [Pitchdeck]. G Data CyberDefense AG.

Harrison, A. A. (1977). Mere Exposure. In *Advances in Experimental Social Psychology* (Bd. 10, S. 39–83). Elsevier. https://doi.org/10.1016/S0065-2601(08)60354-8

Hoyle, R. H. (Hrsg.). (1995). *Structural equation modeling: Concepts, issues, and applications*. Sage Publications.

Hussy, W., Schreier, M., & Echterhoff, G. (2013). *Forschungsmethoden in Psychologie und Sozialwissenschaften für Bachelor: Mit 23 Tabellen* (2., überarbeitete Auflage). Springer.

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11–14. https://doi.org/10.1016/S1361-3723(19)30085-5

Kim, L. (2017). Cybersecurity awareness: Protecting data and patients. *Nursing Management (Springhouse)*, *48*(4), 16–19. https://doi.org/10.1097/01.NUMA.0000514066.30572.f3

Kluge, A., & Gronau, N. (2018). Intentional Forgetting in Organizations: The Importance of Eliminating Retrieval Cues for Implementing New Routines. *Frontiers in Psychology*, *9*, 51. https://doi.org/10.3389/fpsyg.2018.00051

Malhotra, N. K., & Birks, D. F. (2006). *Marketing research: An applied approach* (Upd. 2. European ed). Pearson Education.

Marez, L., Vyncke, P., Berte, K., Schuurman, D., & Moor, K. (2007). Adopter segments, adoption determinants and mobile marketing. *Journal of Targeting, Measurement and Analysis for Marketing*, *16*, 78–95. https://doi.org/10.1057/palgrave.jt.5750057

Mayr, H. C., & Pinzger, M. (2016). *Nophish: Evaluation of a web application that teaches people being aware of phishing attacks*. Gesellschaft für Informatik.

Morgan, S. (2019). 2019 Official Annual Cybercrime Report. *Herjavec Group*, 12.

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., Landesberger, T. von, & Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, 259–284. https://www.usenix.org/conference/soups2020/presentation/reinheimer

Scharf, A., Schubert, B., & Hehn, P. (2015). *Marketing: Einführung in Theorie und Praxis* (6., erweiterte und aktualisierte Auflage). Schäffer-Poeschel Verlag.

Schivinski, B., Christodoulides, G., & Dabrowski, D. (2016). Measuring Consumers' Engagement With Brand-Related Social-Media Content: Development and Validation of a Scale that Identifies Levels of Social-Media Engagement with Brands. *Journal of Advertising Research*, *56*. https://doi.org/10.2501/JAR-2016-004

Shalini Shah, M., Sudhir Diwan, M. D., Lynn Kohan, M. D., David Rosenblum, M. D., Christopher Gharibo, M. D., Amol Soin, M. D., & Adrian Sulindro, M. D. (2020). The technological impact of COVID-19 on the future of education and health care delivery. *Pain physician*, *23*, S367–S380.

Sheth, J. N., & Sisodia, R. (Hrsg.). (2006). *Does marketing need reform? Fresh perspectives on the future*. M.E. Sharpe.

Wong, K. K.-K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, *24*(1), 1–32.