Trust in Cyber Security Recommendations

Johannes Nakayama
RWTH Aachen University
nakayama@comm.rwth-aachen.de

Nils Plettenberg
RWTH Aachen University
plettenberg@comm.rwth-aachen.de

Patrick Halbach
RWTH Aachen University
halbach@comm.rwth-aachen.de

Laura Burbach
RWTH Aachen University
burbach@comm.rwth-aachen.de

Martina Ziefle
RWTH Aachen University
ziefle@comm.rwth-aachen.de

André Calero Valdez
RWTH Aachen University
calero-valdez@comm.rwth-aachen.de

Abstract*— Over the last two decades, the Internet has established itself as part of everyday life. With the recent invention of Social Media, the advent of the Internet of Things as well as trends like "bring your own device" (BYOD), the needs for connectivity rise exponentially and so does the need for proper cyber security. However, human factors research of cyber security in private contexts comprises only a small fraction of the research in the field. In this study, we investigated adoption behaviors and trust in cyber security in private contexts by measuring—among other trust measures—disposition to trust and providing five cyber security scenarios. In each, a person/agent recommends the use of a cyber security tool. Trust is then measured regarding the recommending agent. We compare personal, expert, institutional, and magazine recommendations along with manufacturer information in an exploratory study of sixty participants. We found that personal, expert and institutional recommendations were trusted significantly more than manufacturer information and magazine reports. The highest trust scores were produced by the expert and the personal recommendation scenarios. We argue that technical and professional communicators should aim for cyber security knowledge permeation through personal relations, educating people with high technology self-efficacy beliefs who then disperse the acquired knowledge.

***Index Terms*— Cyber security, human modeling, organizational security, security recommendations, user characteristics**

Introduction

With the advent of the Internet of things and with Internet-ready devices becoming more and more ubiquitous and unavoidable, cyber security gains importance for home and professional users alike. While cyber security software is constantly improving, the weakest link is often the user, e.g., in social engineering attacks. Recent data leaks of personal information have demonstrated the need for safer software systems abundantly [1]. It does not suffice anymore to construct a proper organizational cyber security strategy that only applies to the organization itself. The recent trends towards more devices per person [2] as well as to "bring your own device" (BYOD) [3] have blurred the lines between private and professional networks and require new approaches to cyber security. Outsourcing to third parties and contractors makes this requirement all the more important. The ITRC End-of-Year Data Breach Report 2018 states that a growing number of data breaches are due to subcontractors and third parties, especially in the medical and the educational sector, where they accounted for over 25 % of the records exposed [4].

Yet, data breaches are not the only enhanced risk that arises due to these trends. More and more critical infrastructure is relying on cyber resources, the electrical grid being among the most crucial ones. With growing connectivity, cyberattacks on critical infrastructure become a possibility with potentially devastating consequences [5]. Attacks on IoT devices and infrastructure are increasing [6] and have to be addressed appropriately.

As a consequence, promoting proper cyber security behavior becomes a societal challenge. Furnell, Bryant and Phippen (2007) have shown over a decade ago that there was a lack of cyber security awareness among home users. People seemed to highly overestimate their cyber security expertise and to draw their information from potentially unreliable sources [7]. The most frequent sources of security related information were friends or relatives (41 %), public information or alerting websites (43 %), and IT professionals (43 %). Governmentally funded awareness programmes were among the ones viewed least favorably [7]. In the recent past, cyber security awareness has rather been viewed as an ongoing challenge, as security beliefs have to be updated to new risks constantly [8]. In addition, there is a digital divide between users from different societal strata. Users with higher skills and higher socio-economic status tend to be more aware of cyber security risks due to exposure at the workplace and to access to better resources [9]. Redmiles, Kross and Mazurek (2016) also find that many people rely on trusted people in their surroundings who have a technical background [9].

Even though private user cyber security is of increasing importance, most research focusses on professional users, e.g., in corporations. This is understandable as stakes in professional contexts are usually higher, but it does not justify the lack of research on private user cyber security. The first step to proper cyber security is often the acceptance and adoption of cyber security software. There is a lack of research in this area and we suppose that studying adoption behavior on an individual level might hold some lessons that can be abstracted and applied to professional contexts.

In this study, we investigated how users opt for cyber security software in private contexts. At first, we provide a review of the current research literature: We point out new challenges for cyber security that have implications on the individual as well as on the societal level and review research on human factors that drive cyber security behavior. In the subsequent sections, we describe our methodology, followed by a report of our results. After that, we discuss our findings and close with a conclusion.

Related Work

In this section, we give an overview over the reviewed literature. First, we seek to provide and define the different security-related terms in information systems research. This is the subject of the first paragraph in this section. We then proceed by describing developments that necessitate higher cyber security awareness in the private context. We close this section by providing an overview of the current research literature on human factors and trust in cyber security in private contexts.

I. Information Security, ICT Security, and Cyber Security

Before delving into the subject, it is first important to understand the different concepts that relate to security in information systems contexts because different terms have been used interchangeably in the past. Von Solms and Van Niekerk (2013) provide a distinction between three security-related concepts: information security, information and communication technology (ICT) security, and cyber security [10]. ICT security, in their view, is the protection of the technical system that underlies the organizational structure and constitutes a crucial part of both information and cyber security [10]. However, the latter two concepts go beyond this definition in two ways. The difference between them lies in the protected asset: While information security aims at protecting (confidential) information, cyber security has the goal to protect all entities that are adjacent to the cyberspace (i.e., the users and even society at large). The role of humans is also different in the two constructs: In information security, humans are a vulnerability to the system, whereas in cyber security, they are the asset to be protected [10].

II. Mobile Devices

Cyber security practices have traditionally been developed for stationary infrastructures. With the recent trend towards virtualization and mobile connectivity, however, cyber security is faced with new challenges [11]. Services like cloud computing become more and more commonplace and make it very convenient to work from anywhere at any time and with any device [11]. This creates opportunities for distributed work which in turn calls for new communication tools like Social Media, instant messaging etc. The increasing acceptance of “bring your own device” (BYOD) policies [3] is a logical consequence of these developments. Even though employees could be (and in many cases are) provided with mobile devices for professional purposes specifically, the lines between personal and professional space tend to blur. Many professionals may very well consider using personal devices for work purposes or vice versa out of convenience which is why security needs in this context have to be examined carefully [3]. There is also the possibility of users connecting their personal devices to organizational networks which complicates the enforcement of security standards in organizations [3]. It is unclear if this trend can or should be stopped. Consequently, understanding new attack vectors that arise because of this development is a paramount priority in cyber security research.

III. Social Engineering

The wider spread of mobile devices creates new opportunities for criminal entities who seek to gain access to organizational networks. Social engineering which is defined as “manipulating a person into giving information to the social engineer” [12] is an emergent threat to many organizations and its success has been shown in many major cases such as the Google hack in 2009 [12]. This is why many attack vectors nowadays include users [12].

A common approach to social engineering is “phishing”. Phishing is a practice where the user is directed to a phony website and then incentivized to provide their personal data [13]. In the recent past, social engineers have become more adept in tailoring phishing sites to specific users. A more targeted phishing attack on a specific user is called “spear-fishing” [12]. This can be done either by obtaining information about the user by means of social engineering or by using context-aware spam [12].

Susceptibility to scams of this kind varies on an individual level. Williams, Beardmore and Joinson (2017) provide a framework with which cyber security analysts can evaluate individual susceptibility to online influence. It is comprised by the factors self-awareness, self-control, selfdeception, trust, approach to risk, motivation, and expertise [14].

IV. Cyber-Physical Security Threats

Cyber security has traditionally been focused on mitigating risks concerning the cyberspace. However, with new technologies such as home automation, threats to physical safety through the cyberspace increase [10]. Connectivity is spreading from the cyberspace into the physical world, resulting in the rise of cyber-physical systems. Cyber-physical systems are being used on a small scale (e.g., home automation [15]) as well as on a large scale (e.g., Smart Grid [16]) and come with new security requirements and challenges that go beyond mere cyber security [17][5]. Mo et al. (2012) call this new approach to cyber security in cyber-physical systems *Cyber-Physical Security* [5]. Smaller cyber-physical systems as part of larger systems (e.g., automated homes as part of the Smart Grid) open up the larger systems for attacks through low level entry points [18]. Proper cyber security in private contexts thus becomes paramount as critical infrastructure depends more and more on cyber resources making it more vulnerable to cyberattacks [19].

The electrical grid is arguably the largest engineered system of the world and undoubtedly constitutes critical infrastructure. The vision of making the electrical grid "smart" (thus, building the Smart Grid) aims at making energy management more efficient [17]. However, adding connectivity to the electrical grid comes with major risks that have to be examined carefully before the widespread implementation of a Smart Grid. Sridhar, Hand and Govindarasu (2012) provide an analysis of the coupling between cyber and physical components of the Smart Grid and identify the possible physical impact of an attack as the defining characteristic in the risk assessment for a cyber-physical electrical grid [19]. Attacks on the Smart Grid could indeed prove devastating, especially if it is aimed at the availability of the system (i.e., as a DoS attack) [17][19][5]. A botnet of home automation systems that could have a catastrophic impact on the electrical grid may serve as an exemplary threat [18]. In the worst case, a DoS attack on the electrical grid could result in power outages and damage to the equipment [17]. Furthermore, unwitting users could easily be incriminated in the process [10].

It is not surprising that extensive research has been devoted to technical solutions to this threat as humans will always remain a weakness in cyber security. Wang and Lu (2013) suggest several technical (e.g., rate-limits) as well as cryptographic and protocol related countermeasures to prevent Smart Grid infrastructure from being harmed [17]. Sridhar, Hand and Govindarasu (2012) define technical goals for cyber-physical system security which, among others, are achieving intrusion tolerance and building risk mitigation algorithms [19]. Mo et al. (2012) even make out a supposed weakness of current equipment as a strength: The diversity of embedded firmware could prevent pervasive spread of malware in the Smart Grid [5]. Even though it is very necessary to find technical solutions to mitigate cyber-physical security risks, humans must not be overlooked as a cyber security weakness.

V. Trust and Human Factors in Cyber Security

A crucial factor in cyber security is trust among the agents in a system. Trust (human factor) in this case has to be distinguished from confidence (non-human factor) [20]. Every organization extends different levels of trust to employees creating a hierarchy of trust throughout the organization. As trust is a dynamic phenomenon, it needs to be assessed continuously rather than at one point in time [20]. Trust in organizations is built through user compliance with security policies which has been shown to be an effective means of mitigating cyber security risk [21]. In order to ensure cyber security compliance, employees have to be motivated to comply. An effective motivation measure in this context is collaboration. Safa, Von Solms and Furnell (2016) recommend implementing a culture as well as structures for information security knowledge sharing to motivate employees to comply with security policies [21]. Another way to motivate cyber security compliance is a game-based approach. Different approaches at game-based learning in cyber security have proven effective (e.g., [22]).

To evaluate how trustworthy a user is, it is also important to understand human factors in cyber security. Humans are and will most likely stay the primary target of cyberattacks, so a lack of understanding of human behavior is a common weakness in cyber security systems. Cyber systems are, after all, socio-technical systems and should be treated accordingly [23]. Pfleeger and Caputo (2012) suggest a blend between computer science and behavioral science to achieve more effective cyber security and information security [23]. Bringing together members from the respective research communities could be a promising measure [23]. One such interdisciplinary approach has delivered evidence for an influence of the personality traits conscientiousness and agreeableness from the big five model on the adoption of information security behavior [24].

While there is a plethora of cyber security research in organizational contexts, there seems to be a surprising lack of research on the fringes of cyber security systems, i.e., home users and their cyber security behavior. Even though there are some approaches to heightening cyber security awareness in home users, e.g., through enforcing the use of a mandatory E-Awareness Portal [25], not much effort has been put into understanding the actual behavior of private users. We believe that, regarding the risks that arise due to higher connectivity, especially between physical objects, it is of crucial importance to understand home user cyber security behavior. It has implications even on a societal level and in order to make professional communication more effective, it has to be understood, which human factors drive cyber security behavior in the private context. The following study is an exploratory advance into this area. We try to examine who private users trust when deciding upon a cyber security tool for their private purpose.

METHOD

Measures and variables. To assess the cyber security adoption behavior in private contexts, we constructed an online survey that was conducted from June to August 2017. Alongside demographic variables (age, gender, and education level), we surveyed technology self-efficacy (TSE) [26], disposition to trust (DTT) [27], and structural assurance of the web (SAW) [27]. All scales were assessed on a six-point Likert scale (1 = strongly disagree, 6 = strongly agree). Internal consistency for all scales was acceptable for the analysis ($\alpha_{\mathrm{DTT}} = 0.75$, $\alpha_{\mathrm{TSE}} = 0.86$, $\alpha_{\mathrm{SAW}} = 0.81$). We also asked the participants for their critical decision factor (CDF) when deciding upon a new cyber security software. They were able to choose from the following options: (1) personal recommendations, (2) reviews in magazines, (3) articles on the Internet, (4) previously used software, (5) news, and (6) other.

Subsequently, participants were provided with five scenarios in randomized order:

1) A friend recommends you a security software product. *(personal recommendation)*
2) You read about the National Department for Cyber Security recommending a certain cyber security software product. *(institutional recommendation)*
3) You attend a lecture by a professor for IT security. At the end, she recommends a specific cyber security software product. *(expert recommendation)*
4) You read the manufacturer information of a cyber security software product which explains its benefits in layman’s terms. *(manufacturer information)*
5) You read several reviews on cyber security and find a highly technical explanation of a certain product. *(magazine recommendation)*

For each scenario, the participants had to evaluate, how well the presented software would serve them. For this evaluation, we provided a self-constructed six-point Likert scale that is loosely based on the concepts perceived usefulness, perceived ease of use, and intention to use from the Technology Acceptance Model (TAM) [28], but specified to fit the scenarios at hand. Specifically, the participants had to decide:

- if the recommended software properly protected their computer from unauthorized access,
- if it contained hidden or harmful functionalities,
- if it fit their needs exactly,
- if they deemed it trustworthy (all above map perceived usefulness in the context at hand),
- if they would use the software in the future (intention to use),
- and finally, if it would be easy to install (perceived ease of use).

Internal consistency was excellent for all scenarios $\alpha_{\mathrm{personal}} = 0.91$, $\alpha_{\mathrm{institutional}} = 0.90$, $\alpha_{\mathrm{expert}} = 0.91$, $\alpha_{\mathrm{manufacturer}} = 0.90$, $\alpha_{\mathrm{magazine}} = 0.90$).

Statistical methods. The analysis was conducted in *R* Version 3.5.2 using the package *jmv* [29] and the results were visualized using *ggplot2* [30]. We employed Repeated Measures ANOVA to compare the different scenarios. To test for sphericity, we applied Mauchly’s test. Where appropriate, we applied Greenhouse-Geisser correction to ensure the validity of our results. Post-hoc tests were conducted with Bonferroni corrections. Internal consistency was computed with Cronbach’s α and for correlations, we used Pearson’s *r*. Confidence level was set to 95 % for all measures.

RESULTS

The following section provides the results of our study. The first part is a description of the sample, including the analysis of the influence that the explanatory variables exert on the scenarios. The second part is the main analysis of the differences of the provided scenarios.

I. Sample

Descriptive statistics. Of our 60 participants, 31 were male and 29 were female. The mean age is 26.13 years with a standard deviation of 9.44. This is indicative of a rather young sample which is also reflected in the educational levels: 38 participants reported university entrance level as their highest educational degree, 10 reported a Bachelor’s degree and 9 a Master’s degree. Only three people held different degrees or were educated otherwise. The participants’ disposition to trust ($M = 3.90$, $SD = 0.63$), their technology self-efficacy beliefs ($M = 4.00$, $SD = 0.82$), and their structural assurance of the web ($M = 4.03$, $SD = 0.91$) were rather high.

Interestingly, our participants preferred personal recommendations (36.67 %) over any other recommendation source. The distribution can be seen in Figure 1. Two of the three participants who chose “other” wanted to choose more than one option and one person stated that they did not use cyber security software.

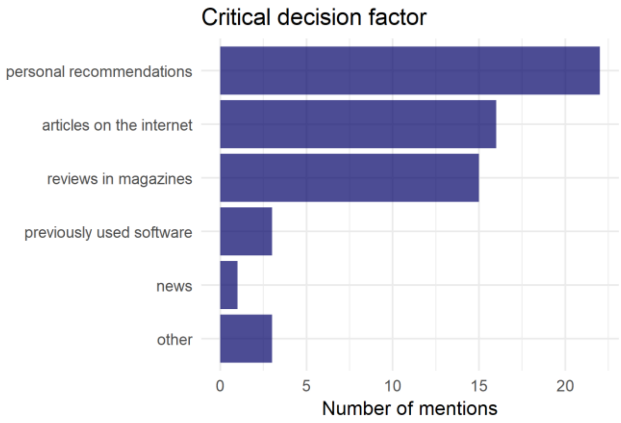

FIGURE 1. CRITICAL DECISION FACTOR. MOST IMPORTANT FACTORS IN THE DECISION FOR A CYBER SECURITY SOFTWARE.

Influence of explanatory variables. There are several considerable correlations between the explanatory variables and the user evaluation for the different scenarios. Disposition to trust and structural assurance of the web are significantly positively correlated with the scores from the personal, institution, and expert scenario. Technology self-efficacy is significantly positively correlated with the scenario in which participants got the recommendation from the manufacturer information. The correlations are displayed in Table 1. There is also a moderate correlation between the explanatory variables disposition to trust and structural assurance of the web ($r(58) = 0.45$, $p < .001$).

TABLE 1. CORRELATIONS. CORRELATION MATRIX FOR EXPLANATORY VARIABLES AND SCENARIOS.

	DTT	**SAW**	**TSE**
personal	0.38**	0.43***	0.04
institution	0.46***	0.45***	0.04
expert	0.33*	0.35**	-0.07
manufacturer	0.10	0.22	0.32*
magazine	0.13	0.12	0.24

II. Differences between the Scenarios

Mauchly's test for sphericity indicates that the assumption of sphericity has been violated ($p < .001$) which is why Greenhouse-Geisser correction was applied. There is a significant effect of the recommendation scenario on users' trust in the recommendation ($F(3.19, 187.93) = 40.7$, $p < .001$). The effect size is $\eta^2_{\text{part}} = .408$. The post-hoc comparisons using t-test with Bonferroni correction show significant differences between several scenarios. The results can be seen in Table 2. The scenarios roughly group together in two groups (*group 1*: friend, institution, expert, *group 2*: manufacturer, magazine) that are significantly different from each other. In addition, there is a significant difference between the expert and the institution scenario, with the expert scenario scoring significantly higher. The results are visualized in Figure 2 ($M_{\text{personal}} = 4.46$, $SD_{\text{personal}} = 0.85$, $M_{\text{institution}} = 4.19$, $SD_{\text{institution}} = 1.02$, $M_{\text{expert}} = 4.53$, $SD_{\text{expert}} = 0.91$, $M_{\text{manufacturer}} = 3.44$, $SD_{\text{manufacturer}} = 0.95$, $M_{\text{magazine}} = 3.58$, $SD_{\text{magazine}} = 0.93$).

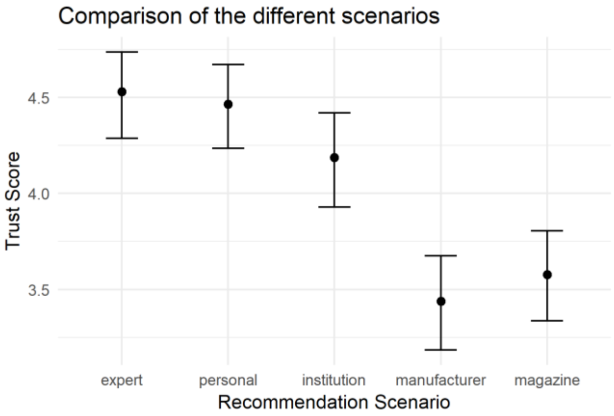

FIGURE 2. CONFIDENCE INTERVALS. MEANS AND CONFIDENCE INTERVALS FOR THE DIFFERENT SCENARIOS.

DISCUSSION

The source of a recommendation seems to matter in cyber security adoption. Personal recommendations as well as expert and institutional recommendations have an edge over magazine recommendations and manufacturer information. Generally, people in our sample seem to be more concerned about the source than the contents of the recommendation which is in line with previous findings [7]. The manufacturer information as well as the magazine scenario were the only ones that contained mildly or highly technical information respectively. It is also conceivable that participants were deterred by the information because they did not understand it. Furthermore, it is interesting to note that the expert and the personal scenario produced the highest trust scores among the scenarios with institution as a close third. In both former cases, a person gives the recommendation which appears to be a driving factor for trust.

In addition to the differences between the scenarios, there were significant effects of the explanatory variables on certain scenarios. Disposition to trust and structural assurance of the web are highly positively correlated with the personal, institution and expert scenario. People with a higher disposition to trust tend to rely on other people more [27] and it is not surprising that this applies to recommendations on cyber security software as well.

TABLE 2. DIFFERENCES. POST-HOC COMPARISON OF THE SCENARIOS.

Scenarios		**Mean Difference**	***SE***	***df***	***t***	***p*-bonferroni**
personal	– institution	0.278	0.112	236	2.482	.137
	– expert	-0.067	0.112	236	-0.598	> .999
	– manufacturer	1.026	0.112	236	9.177	< .001***
	– magazine	0.886	0.112	236	7.923	< .001***
institution	– expert	-0.344	0.112	236	-3.080	.023*
	–manufacturer	0.749	0.112	236	6.694	< .001***
	– magazine	0.608	0.112	236	5.440	< .001***
expert	– manufacturer	1.093	0.112	236	9.774	< .001***
	– magazine	0.953	0.112	236	8.520	< .001***
manufacturer	– magazine	-0.140	0.112	236	-1.254	> .999

They also seem to extend this trust to institutions and experts. Belief in professional people doing a good job is explicitly part of the disposition to trust scale which might be the reason for the high trust in expert recommendations. The "Bundesamt für Sicherheit in der Informationstechnik" (BSI) that was used for the institution scenario might have skewed the trust favorably because it is a well-established governmental organization. Lesser known institutions might have produced different results. In further research, this can be tested by providing people with recommendations from different institutions. Furthermore, not just the author of the recommendation plays a role in acceptance, but also content and required information for the recommendation [31]. Friends, who received high ratings in our study, might be more familiar with the individual situation and thus more "private" and relevant for giving recommendations. Structural assurance of the web is an uncertainty factor that might undermine trust in certain people who are very insecure on the web. However, disposition to trust and structural assurance of the web have a reasonably high positive correlation which is indicative of people with higher disposition to trust also having a high structural assurance of the web. Participants with higher technology self-efficacy beliefs displayed higher trust in manufacturer information that was moderately technical. The implication of this finding is that people want to understand the software that they are using and people with higher technology self-efficacy beliefs might possess higher expertise in addition to their higher beliefs in their ability to handle the software. All of these findings can be applied to improve strategies to heighten cyber security awareness. Technical and professional communicators could target people with high technology self-efficacy beliefs and educate them about cyber security. As social networks tend towards a power law node distribution [32] and to bundle into tightly networked communities [33], the diffusion of knowledge through social networks should not be underestimated. Our findings as well as previous work show that friends or acquaintances are an important source for recommendations on cyber security software. A potential challenge could be to reach people with low disposition to trust and structural assurance of the web. However, those people might still trust friends' advice more than institutional advice, which is why, in addition to public information, propagating cyber security knowledge through social networks should be a focus of technical communicators. Even though the inclination to trust personal recommendations over any other recommendations can be used to propagate proper cyber security software and practices, it can be used to achieve the opposite as well. Trusting any recommendations is not helpful if the people who recommend a certain software or practice are ill-advised themselves. It is thus very important that technical communicators in cyber security find ways to establish themselves as experts and to distinguish themselves from phony advisors. How this can be done is an open research issue that is out of the scope of this study. However, based on the findings of this study, an inquiry into how expert status is perceived by people might be worthwhile. If cyber security experts found non forgeable ways to gain the trust of influencers (who could then permeate the knowledge further), bad advice could be exposed as such much easier.

CONCLUSION

In this study, we addressed the lack of research aimed at understanding private user cyber security behavior. Specifically, we investigated who private users trust when deciding upon cyber security software for their private use. We found evidence that users trust personal, expert and institutional recommendations more than magazine recommendations and manufacturer information. From that, we derived possible measures that could be taken to increase public cyber security awareness through professional communication. We hope that our research provides a useful look into initial cyber security adoption behavior in private contexts and that professional communicators may find it useful to design strategies to heighten cyber security awareness.

ACKNOWLEDGEMENTS

We would like to thank our reviewers for their helpful comments on this study. We would further like to thank the people who took the time to participate in this study.

REFERENCES

[1] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid, “Data Exfiltration: A Review of External Attack Vectors and Countermeasures”, *Journal of Network and Computer Applications,* vol. 101, pp. 18-54, 2018.

[2] B. Safaei, A. M. H. Monazzah, M. B. Bafroei, and A. Ejlali, “Reliability Side-Effects in Internet of Things Application Layer Protocols”, in 2nd *International Conference on System Reliability and Safety*, 2017, pp. 207-212.

[3] K. W. Miller, J. Voas, and G. F. Hurlburt, “BYOD: Security and Privacy Considerations”, *IT Professional*, vol. 14, no. 5, pp. 53-55, 2012.

[4] ITRC, “End-of-Year Data Breach Report 2018”, Identity Theft Resource Center, 2019.

[5] Y. Mo *et al.*, “Cyber-physical Security of a Smart Grid Infrastructure”, *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, 2012.

[6] Symantec, “Internet Security Threat Report, Volume 24”, Symantec Enterprise Security, 2019.

[7] S. M. Furnell, P. Bryant, and A. D. Phippen, “Assessing the security perceptions of personal Internet users”, *Computers & Security*, vol. 26, no. 5, pp. 410-417, 2007.

[8] J. Abawajy, “User preference of cyber security awareness delivery methods”, *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237-248, 2014.

[9] E. M. Redmiles, S. Kross, and M. L. Mazurek, “How I Learned to be Secure: A Census-Representative Survey of Security Advice Sources and Behavior”, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 666-677.

[10] R. Von Solms and J. Van Niekerk, “From information security to cyber security”, *Computers & Security*, vol. 38, pp. 97-102, 2013.

[11] D. Kolevski and K. Michael, “Cloud Computing Data Breaches A socio-technical review of the literature”, in *Proceedings of the 2015 International Conference on Green Computing and Internet of Things*, 2015, pp. 1486-1495.

[12] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks”, *Journal of Information Security and Applications*, vol. 22, pp. 113-122, 2015.

[13] R. Dhamija, J. Tygar, and M. Hearst, “Why Phishing Works”, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2006, pp. 581-590.

[14] E. J. Williams, A. Beardmore, and A. N. Joinson, “Individual differences in susceptibility to online influence: A theoretical review”, *Computers in Human Behavior*, vol. 72, pp. 412-421, 2017.

[15] L. Jiang, D.-Y. Liu, and B. Yang, “Smart Home Research”, in *Proceedings of 2004 International Conference on Machine Learning and Cybernetics*, 2004, vol. 2, pp. 659-663.

[16] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart Grid—the New and Improved Power Grid: A Survey”, *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944-980, 2012.

[17] W. Wang and Z. Lu, “Cyber security in the Smart Grid: Survey and challenges”, *Computer Networks*, vol. 57, no. 5, pp. 1344-1371, 2013.

[18] C. Neuman, “Challenges in Security for Cyber-Physical Systems”, in *DHS Workshop on Future Directions in Cyber-Physical Systems Security*, 2009, pp. 22-24.

[19] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber-physical System Security for the Electric Power Grid”, *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, 2012.

[20] D. Henshel, M. Cains, B. Hoffman, and T. Kelley, “Trust as a human factor in holistic cyber security risk assessment”, *Procedia Manufacturing*, vol. 3, pp. 1117-1124, 2015.

[21] N. S. Safa, R. Von Solms, and S. Furnell, “Information security policy compliance model in organizations“, *Computers & Security*, vol. 56, pp. 70-82, 2016.

[22] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, “A video game for cyber security training and awareness”, *Computers & Security*, vol. 26, no. 1, pp. 63-72, 2007.

[23] S. L. Pfleeger and D. D. Caputo, “Leveraging behavioral science to mitigate cyber security risk”, *Computers & Security*, vol. 31, no. 4, pp. 597-611, 2012.

[24] J. Shropshire, M. Warkentin, and S. Sharma, “Personality, attitudes, and intentions: Predicting initial adoption of information security behavior”, *Computers & Security*, vol. 49, pp. 177-191, 2015.

[25] E. Kritzinger and S. H. von Solms, “Cyber security for home users: A new way of protection through awareness enforcement”, *Computers & Security*, vol. 29, no. 8, pp. 840-847, 2010.

[26] G. Beier, *Kontrollüberzeugungen im Umgang mit Technik: Ein Persönlichkeitsmerkmal mit Relevanz für die Gestaltung technischer Systeme*. dissertation.de, 2003.

[27] D. H. McKnight, V. Choudhury, and C. Kacmar, “Developing and Validating Trust Measures for e-Commerce: An

Integrative Typology“,*Information Systems Research*, vol. 13, no. 3, pp. 334-359, 2002.

[28] V. Venkatesh and F. D. Davis, “A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies“, *Management Science*, vol. 46, no. 2, pp. 186-204, 2000.

[29] R. Selker, J. Love, and D. Dropmann, *jmv: The 'jamovi' Analyses*. 2018 [Online]. Available: https://CRAN.R-project.org/package=jmv

[30] H. Wickham, *ggplot2: Elegant Graphics for Data Analysis*. Springer-Verlag New York, 2016 [Online]. Available: http://ggplot2.org

[31] L. Burbach, J. Nakayama, N. Plettenberg, M. Ziefle, and A. Calero Valdez, “User preferences in recommendation algorithms: The influence of user diversity, trust, and product category on privacy perceptions in recommender algorithms“, in *Proceedings of the 12th ACM conference on Recommender Systems*, 2018, pp. 306--310.

[32] A.-L. Barabási and R. Albert, “Emergence of Scaling in Random Networks“, *Science*, vol. 286, no. 5439, pp. 509-512, 1999.

[33] M. Girvan and M. E. Newman, “Community structure in social and biological networks“, *Proceedings of the National Academy of Sciences of the United States of America*, vol. 99, no. 12, pp. 7821-7826, 2002.

About the Authors

Johannes Nakayama (B. Sc.) is a student assistant at the chair for communication science at RWTH Aachen University and a part of the junior research group ‘Digitale Mündigkeit’. He is a Master’s student majoring in technical communication (communication science and computer science) and he specializes in recommender systems research.

Nils Plettenberg (B. Sc.) works as student assistant at the chair for communication science at the RWTH Aachen University, Germany where he is part of the junior research group ‘Digitale Mündigkeit’. He is studying the master’s program electrical engineering with a major in computer engineering. His research focuses on the spread of news in social media.

Patrick Halbach (M. Sc.) works as research assistant at the chair of Communication Science at RWTH Aachen University, Germany and is part of the junior research group ‘Digitale Mündigkeit’. In his research, he currently deals with opinion formation in online contexts, especially focusing on the impact of social media and the spread of misinformation on such platforms.

Laura Bubach (M.A.) is research assistant at the Human-Computer Interaction Center. Since 2018 she is part of the junior research group ‘Digitale Mündigkeit’. She is currently investigating whether and to what extent different recommendation systems, voice assistants and individuals are accepted by users of social media. Besides her research focuses on target groups of Life-Logging.

Martina Ziefle is Professor of Communication Science and head of the Human Computer Interaction Center of RWTH Aachen University. Her research focuses on the interface between humans and technology, taking into account different usage contexts and user requirements. She focuses in particular on the sensitive area of eHealth technologies, in which user diversity and technology acceptance play a decisive role.

André Calero Valdez (PhD) is junior research group leader at the RWTH Aachen University, Germany. His research focuses the interaction of humans and algorithms such as recommender systems, information visualization, and machine learning in a wide variety of applications. The fields of application range from social media over health informatics to industry 4.0.