Cybersecurity-related behavior of personnel in the Norwegian industry*

Kristian Kannelønning[0000−0002−1480−0709] and
Sokratis Katsikas[0000−0003−2966−9683]

Norwegian University of Science and Technology, Department of Information Security and Communication Technology, Gjøvik 2815, Norway
{kristian.kannelonning, sokratis.katsikas}@ntnu.no
https://www.ntnu.edu/iik

Abstract. Information security policies are formalized rules and regulations that employees should follow to avoid unwanted cyber incidents. This paper reports on the findings of a survey among personnel employed in the Norwegian industrial sector. The survey measured how the respondents self-assess their risky behavior and cognitive awareness regarding the importance and likelihood of cyber security events. A modified version of the Behavioral Cognitive Internet Security Questionnaire was used as the survey instrument. The results indicate that the employees in the target group have a low level of risky behavior and a high level of cognitive awareness and that minimal discrepancy between how respondents self-assess and act in the simulation exists. The result should be of interest to practitioners in the field of cybersecurity since training is attributed as the main driver of the obtained results. Furthermore, strong indications exist that the selected literature and theory do not hold true for the Norwegian industry sector.

Keywords: cybersecurity behavior · IT and OT personnel · Norwegian industry

1 Introduction

The materialization of industry 4.0, where increased interconnectivity leads to more production, simplicity, and ease of use, opened up an abundance of new attack vectors. With new advanced technology deployed in an environment with historically low-security awareness, the chances of successful cyberattacks have increased [11]. As humans are the weakest link in information security [9], and technology cannot be the single solution for security [21], organizations should be able to assess the cybersecurity-related behavior of their employees so as to inform and focus their cybersecurity policies and practices, including those on

* This work has been funded by the Research Council of Norway under grants 323131 (How to improve Cyber Security performance by researching human behavior and improve processes in an industrial environment) and 310105 (SFI Norwegian Centre for Cybersecurity in Critical Sectors - NORCICS)

staff awareness and training. To this end, this paper reports on the findings of a survey among personnel employed in the Norwegian industrial sector using a modified version of the Behavioral Cognitive Internet Security Questionnaire (BCISQ) [17].

The remaining of the paper is structured as follows: Section 2 provides a short overview of the relevant literature. Section 3 presents the hypotheses that were tested with the survey, section 4 describes our methodology, section 5 presents, analyzes, and discusses the findings and, finally, section 6 summarizes our conclusions.

2 Related work

To assess and measure employee behavior, surveys are the most used tool. A recent literature study [20] showed that over 90% of the assessments related to cybersecurity behavior are performed through a self-assessment questionnaire, most commonly the Human Aspects of Information Security Questionnaire (HAIS-Q), developed by [12]. Surveys are fitting when researchers want to extract information directly from people about what they think, believe, and know [4], [22]. The use of self-assessment questionnaires does, however, have a potential pitfall: the respondents' answers could be biased. Response biases exist in the current scales used to measure security policy compliance [10]. It is, therefore, essential to extend or include some form of observational data in addition to self-assessment to assess actual compliance. One way to check actual behavior is through simulations of actual behavior embedded within a questionnaire. The BCISQ, developed by Velki et al. [17], is a validated questionnaire with four simulations that measure self-assessed and actual behavior.

Our earlier work [20] suggests that *"...future research should address the problem of objectively assessing cybersecurity-related behavior and the factors affecting it* and that the research gap on *"...whether there exist differences between manager and employee behavior* should be addressed. Additionally, as called for by [18], the BCISQ should be tested in other cultures and age groups than already tested. Accordingly, this study utilizes a modified BCISQ for a targeted audience, namely managers and employees working with IT and OT within the Norwegian industrial sector.

3 Hypotheses

According to [13], managers have a significantly lower level of Information Security Awareness (ISA) than regular staff. This difference could affect the organization significantly since management plays a critical part in building the organization's security culture. Therefore the following hypothesis will be tested:

- H_1: Management is expected to be less risk-averse and aware than regular employees.

Employees' perception or ability to perceive risk accurately will influence their behavior. Individuals who understand the risks associated with information security are more likely to act appropriately [12]. People may perceive a relatively high possibility of being exposed to a threat if they have already been exposed in the past. Therefore, employees in organizations that have been victims of a cyberattack would have a better understanding of risk. Hence the following hypothesis will be tested:

- H_2: It is expected that employees working in organizations who have been victims of cyberattacks to be more risk-averse and aware than employees in organizations not yet victims of cyberattacks.

Huang et al. [6] found that knowledge also plays a significant part in people's understanding of threats and in their behavior. Further, it is often difficult to understand some security risks without technical knowledge [12]. Employees working within OT most often have some technical education and are expected to have better technical knowledge than other groups. Therefore the following hypothesis will be tested:

- H_3: Employees working primarily with OT are expected to be more risk-averse and aware than non-OT personnel.

4 Methodology

4.1 The survey instrument

The latest iteration of the BCISQ [16] consists of four different scales, specifically two *behavior* scales (a *self-assessment* one and a *simulation* one), and two *cognitive* scales. The behavior scale measures risky online behavior through both self-assessment and simulations of actual online behavior. The behavioral simulation consists of four (k=4) simulations and four self-assessment questions (k=4). The two cognitive scales measure users' information security awareness regarding risk (k=5) and awareness concerning importance (k=4).

In preparation for deployment, 21 faculty members and employees within industry tested the survey questionnaire. These tests resulted in several minor and two significant changes to the original BCISQ. The final version consisted of 24 questions, with three additional questions depending on some responses, resulting in a maximum of 27 questions. These include qualifying questions such as age and length of employment, and participants were asked to self-determine their current role, e.g., if they primarily work with OT or non-OT. The significant changes were on the behavioral simulation and cognitive awareness risk scales. The behavior simulation scale, that initially consisted of k=4 items, was reduced to k=1. The reason for altering the simulations is related to the deployment method of the survey. The original BCISQ asked for the respondent's email; this would be superfluous in our case when the email addresses of the respondents are already known. The cognitive scale regarding risk was

changed following feedback from the test group: the test group reported that the interpretation of the term *risk* was ambiguous. Risk can be described as $Risk = Likelihood * Impact$ [2]. Hence, one may focus on one of the two constituents of risk rather than on both. To resolve this ambiguity, the term *risk* was replaced by the term *likelihood*. The questionnaire used in the survey can be accessed at https://nettskjema.no/a/338436.

Before distributing the survey, the questionnaire was submitted for approval to and was approved by the Norwegian Data Protection Authority.

4.2 Sample selection and distribution

The survey was distributed to 577 recipients by a personalized email, where a link to the survey was provided. The survey questionnaire was hosted at https://nettskjema.no. Participants were identified from prior contact with one of Norway's largest suppliers of industrial equipment. All 577 recipients were contacted by a cold email, i.e., no prior contact had been made between the researchers and the recipients. Included in the text were clearly stated selection criteria for participation: The respondents should be employed in a Norwegian organization or department that primarily operates within the industrial sector or with industrial applications, i.e., the recipients employed at hospitals were from the technical department of the organization. Included in the invitation were a declaration from the Norwegian Data Protection Authority informing participants of the approval of the study, a consent form, data storage information, and their legal rights as participants.

The personalized email received 63 responses before a follow-up email was sent about two weeks later, fetching another 50 responses. The survey was open for about five weeks in January-February 2023. Of the 577 survey invitations, 94% were sent to males and 6% to females.

Employees from 182 different organizations were invited to the survey. In the qualifying questions for this survey, questions about company size and primary business were excluded to keep the survey as short as possible. Instead, an analysis based on the email domain has been conducted to unveil what the organizations have reported as their primary business to the Norwegian official registrars [3]. Of the organizations, only 21 or 12% have been classified as multinational, meaning they have offices or subsidiaries in multiple countries. This does not mean that organizations not included in the 21 accounted for do not operate or sell goods outside Norway, but they do not indicate offices outside Norway. The organizations have been categorized as shown in Table 1. Table 2 presents the size of organizations based on the number of employees and invitations sent to each size bracket.

5 Findings

5.1 Collected data

In total 113 responses were received; this only counts surveys that were fully completed. These correspond to a response rate of 19,5%, with an average time

Table 1. Classification of the 182 organizations into sectors and percentage of survey invitations sent to each category.

Sectors based on organizations' self-reported primary activity	Percentage of invitations
Technical consultants	14,8%
Production of Oil & Gas	1,6%
Production of raw materials or goods	15,4%
Processing and production of food	6,6%
Production of machines	13,2%
Wholesales of Industrial Equipment	12,1%
Hospitals (technical personnel)	2,2%
Service and maintenance to Industry	18,1%
Software development companies	4,9%
Other	11%

Table 2. Size of organizations based on the number of employees and invitations sent to each size bracket.

Number of employees	Companies in each size bracket	Invitations sent
1-4	7	1,5%
5-9	7	2,7%
10-19	26	12,4%
20-49	31	17,9%
50-99	34	15,4%
100-249	23	13,7%
250 - 499	22	19,6%
500 - 999	12	4,6%
1000 - above	20	12,4%

to complete the survey of 7 minutes, 14 seconds, and a median of 5 minutes and 19 seconds. The survey tool did not track the number of survey responses that were started but not completed. The respondents were 95,6% (n=108) male and 4,4% (n=5) female. Statistics Norway (ssb.no) reports that 83% of males and 17% of females are employed in the target group. However, these numbers include all employees, whereas this study has targeted more technical personnel. 56,6% (n=64) report that they primarily work with Operational Technology; of those, as many as 40,6% work with engineering, a male-dominated occupation. Of the 113 participants, 45,1% (n=51) report having managerial duties, i.e., someone reporting to them, and 42,5% (n=48) report that their organization has been affected by a cyberattack. The age groups 46-50, 51-55, and 56-60 account each for 20,4% of the responses. The age group 46 – 60 represents 61,2% of the participants. The remaining 38,8% are distributed as follows: 26-30y: 1,8%, 31-35y: 2,7%, 36-40y: 8,8%, 42-45y: 15,9%, 61-65y: 8,8% and 66-70y: 0,9%.

5.2 Analysis

The Cronbach α was calculated to check the responses for internal consistency [15]. Values above 0,7 are deemed acceptable [5], [8], [15]. The Cronbach α for

all 13 items, including behavior self-assessment, k=4, and cognitive awareness, k=9, was found to be $\alpha = 0,715$. When dividing the two scales, the behavioral self-assessment scale with only four questions gives $\alpha = 0,278$, indicating a low or unacceptable internal consistency. However, the value of α partly depends on the number of items on the scale. A low α might result from too few items in the scale [5], [8], [15]. For the cognitive awareness, k=9, $\alpha = 0,713$.

The descriptive statistics shown in Table 3 show that respondents show a low level of risky online behavior and a high level of cognitive awareness towards the importance of, e.g., regularly updating devices. A low value for the self-assessment behavioral scale would indicate a low level of risky behavior. A high value for the Cognitive awareness scale would indicate that respondents have a high self-assessed awareness of the importance and likelihood of internet security. In comparison, the respondents are placed mid-range on questions about likelihood, as for example reflected in the responses to the question *"How would you rate the likelihood of someone hacking your personal computer, laptop, or smartphone?"*

Table 3. Descriptive statistics n=113.

BCISQ Subscales	Min	Max	MEAN	SD
Risky behavior self-assessment scale	1	2	1,14	0,38
Cognitive importance scale	2,5	5	4,22	0,92
Cognitive likelihood scale	1	4,2	2,46	0,87

To test the three hypotheses stated in Section 3, a one-way analysis of variance (ANOVA) was performed. The results are shown in Table 4.

Table 4 shows that all three hypotheses have a $p > 0,05$ and their F-values are within F-critical. Therefore, no difference within each group is found, and we do not reject any null hypothesis; there is no difference between groups as H_1, H_2, and H_3 hypothesize.

The final question on the survey was the behavior simulation, k=1. The simulation is designed to test the participants in an actual situation and see if they would willingly reveal private data. The simulation asked the following: *To check the quality of your password security, please write down your most used password.* Of the n=113, the vast majority, n=102 (90%), either did not respond or responded with something obviously not their password, e.g., *1youwillnotget-mypassword!:)*. However, n=7 (6%) revealed what is believed to be their most used password, and n=4 (4%) revealed something that resembles a password but might not be their most used one. Standard password rules were applied to analyze the submitted passwords. A chi-square analysis was performed to see if there was a difference between those who provided their most used password and their role as management or employee. The chi-square, $x^2 = 0,83, CV = 3,84$, and $p = 0,36$ shows no difference between the participants' position and their inclination to reveal their password. Furthermore, all participants were asked *How would you rate your general technical knowledge about computers and the*

Table 4. One-way ANOVA.

			N	MEAN	SD	P/F/F-crit
	Behavior	Management	51	1,20	0,42	
H_1		Employees	62	1,10	0,34	
						0,53/0,40/3,93
	Awareness	Management	51	3,19	1,23	
		Employees	62	3,28	1,26	
	Behavior	Victims	48	1,16	0,40	
H_2		Non-victims	65	1,13	0,36	
						0,56/0,34/3,93
	Awareness	Victims	48	3,21	1,21	
		Non-victims	62	3,26	1,28	
	Behavior	OT	64	1,15	0,38	
H_3		Non-OT	49	1,14	0,39	
						0,67/0,18/3,93
	Awareness	OT	64	3,25	1,21	
		Non-OT	49	3,22	1,30	
	Behavior	Total	113	1,14	0,38	
	Awareness	Total	113	3,24	1,25	

internet? on a four-point scale from Poor, Fair, Good, and Excellent. Of the n=113, 18% reported having excellent knowledge, 67% Good, 13% Fair and 2% Poor. Those who revealed their password (n=7) reported either good (n=3), or fair (n=4) knowledge. When examining the difference between the groups (those who revealed their password and those that did not), and how they self-assess their knowledge, the results were $x^2 = 12,93$, $CV = 7,81$, and $p = 0,0047$. This means that there is a statistical difference between the groups and how they self-assess their knowledge. i.e., a low self-assessment of one's knowledge will increase the probability of unintentionally revealing one's password. No statistical difference was found in the self-assessment of those within the group that did reveal their password. Ergo, they self-evaluate their behavior and awareness, similar to the ones who did not reveal their password. Their intention to comply is the same, but their knowledge level differs from those who passed the test. Of the group self-defining as having excellent knowledge, as many as 80% work within OT. Although no difference between OT and non-OT personnel was found ($x^2 = 7,62$, $CV = 7,81$, and $p = 0,055$), the results are very close to revealing a difference between how OT and non-OT personnel self-assess their general technical knowledge about computers and the internet.

5.3 Discussion

The overall results for the self-assessment align with those given in [19]. The mean for the behavioral scale indicates that respondents have a low level of risky behavior. However, whereas [19] produced similar levels of self-assessed behavior, they still received passwords from 45,5% of the respondents. The participants in that study were psychologists with assumed expertise in the field

of behavioral science with some work experience in the internet security area. In another study, with students as participants, [19] received passwords from 38,4%. Our study only received what is believed to be the most used password from 6% of the participants, meaning that the participants employed within the Norwegian industry act more in accordance with how they self-evaluate their behavior than previous studies have shown. No difference in self-assessment between those who revealed their password and the majority who did not reveal their password was found. The only statistical difference was the assessment of their technical knowledge. All who gave away their personal information rated their knowledge level only as good or fair. This positive deviation from [19] could be the result of differences in training. In our study, as many as 71% report that they have received training concerning IT security. Furthermore, 88,5% report that their organization has a security policy, and 79% report that they are either familiar or very familiar with the policy's content.

According to [13], management has a much lower ISA than regular staff. However, we found no difference in behavior between managers and employees. The result should be positively viewed because managers are responsible for culture and building a positive security culture. The fact that users report their behavior and awareness similarly even without the experience of working in an organization that has been a victim of a cyberattack and even without the benefit of additional technical knowledge would at least indicate that the training and culture in the included organizations have influenced the recipient's behavior. H_3 hypothesized that there exists a difference between OT and non-OT employees. H_3 was also rejected; however, an interesting finding is that OT personnel rate their knowledge differently than non-OT personnel do. x^2 did not show statistically a difference, but the results are very close to $p < 0,05$, meaning that the hypothesis was not unreasonable.

Using simulations in a survey is a simple and cost-effective way of testing actual behavior. However, asking for a password might be too obvious, considering that 71% have received training that most likely includes the topic of sharing passwords. However, receiving any password is, of course, not good, and one is one too many. As a mitigating effect, it should be pointed out that the email with the survey was sent from a credible university account with verifiable information, and the survey was hosted on a legitimate website operated by a university. Every aspect of the communication and the procedure was credible and written in perfect Norwegian. This seems to confirm that trust in the sender (or alleged sender) is significant in falling for a phishing attack.

The survey fetched a decent response rate, given the deployment method of cold emails. Some of the reasons might be the length of the survey. Respondents were informed that it took less than 6 minutes to complete, a doable extra task in a hectic work week. So, while the BCISQ has the benefit of length and has been validated by its authors, this research should, in hindsight, have developed more simulations to test the respondents further and more intelligently than only asking for their password. Having just one simulation that might be too obvious for many could hinder capturing actual behavior.

6 Conclusion

The study produced promising results. The respondents show a low level of risky behavior when self-assessed and simulated. Furthermore, the respondents show a high level of awareness regarding the importance of cybersecurity. The finding that all three of our hypotheses are rejected also speaks in favor of organizations. Leveling out the differences between management and employees, between those with self-reported excellent technical knowledge, and between employees from organizations who have experienced cyberattacks and those that have not indicate that organizations have reached a favorable position where no one group is significantly weaker. This research has not investigated how these organizational results have been obtained, but considering the relatively high degree of training and the high familiarity with the organizations' security policy could indicate that the efforts done by Norwegian industry to educate employees in information security is working. Our future research aims at investigating these issues further.

References

1. Ajzen, I.: The theory of planned behavior. Organizational Behavior and Human Decision Processes **50**(2), 179–211 (1991)
2. Cox, A. L. Jr: What's wrong with risk matrices?. Risk Analysis: An International Journal **28**(2), 497–512 (2008)
3. The Brønnøysund Register Centr, https://w2.brreg.no/enhet/sok/index.jsp. Last accessed 17 Apr 2023
4. Fink, A.: How to conduct surveys: A step-by-step guide. Sage Publications, (2015)
5. Gliem J.A., Gliem R.R.: Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales. In: 2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education, pp. 82–88. Columbus OH, USA (2003)
6. Huang, DL., Rau, PL.P., Salvendy, G.: A Survey of Factors Influencing People's Perception of Information Security. In: Jacko, J.A. (eds) Human-Computer Interaction. HCI Applications and Services. HCI 2007. LNCS, vol, 4553, pp 906—915. Springer, Berlin, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73111-5_100
7. Jalali, M. S., Bruckes, M., Westmattelmann, D., Schewe, G.: Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. Journal of medical Internet research **22**(1), e16775 (2020)
8. Kocak, C., Egrioglu, E., Yolcu, U., Aladag, C. H.: Computing Cronbach alpha reliability coefficient for fuzzy survey data. American journal of intelligent systems **4**(5), 204–213 (2014)
9. Kruger, H., Toit, T. d., Drevin, L., Maree, N.: Acquiring sentiment towards information security policies through affective computing. In: Proceedings 2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), pp. 1–6. IEEE Press, New York City (2020)
10. Kurowski, S.: Response biases in policy compliance research. Information & Computer Security **28**(3), pp. 445–465 (2019)

11. Oueslati, N. E., Mrabet, H., Jemai, A., Alhomoud, A.: Comparative Study of the Common Cyber-physical Attacks in Industry 4.0. In: Proceedings 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), pp. 1–7. IEEE Press, New York City (2019)
12. Parsons, K., McCormac, A., Butavicius, M., Ferguson, L.: Human factors and information security: individual, culture and security environment. Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation, Edinburgh South Australia 5111, Australia (2010)
13. Reeves, A., Parsons, K., Calic, D.: Whose Risk Is It Anyway: How Do Risk Perception and Organisational Commitment Affect Employee Information Security Awareness?. In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2020. LNCS, vol 12210. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-50309-3_16
14. Serpanos, D.: The cyber-physical systems revolution. Computer **51**(3), 70–73 (2018)
15. Vaske, J. J., Beaman, J., Sponarski, C. C.: Rethinking Internal Consistency in Cronbach's Alpha. Leisure Sciences **39**(2), 163–173 (2017)
16. Velki, T.: Psychologists as information-communication system users: Is this bridge between information-communication and behavioral science enough to prevent risky online behaviors?. In: Proceedings of 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), pp. 1048–1052. IEEE Press, New York City (2022)
17. Velki, T., Mayer, A., Norget, J.: Development of a New International Behavioral-Cognitive Internet Security Questionnaire: Preliminary Results from Croatian and German samples. In: Proceedings of 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1209–1212. IEEE Press, New York City (2019)
18. Velki, T., Šolić, K.: Development and validation of a new measurement instrument: The behavioral-cognitive internet security questionnaire (BCISQ). International journal of electrical and computer engineering systems **10**(1.), 19–24 (2019)
19. Velki, T., Šolić, K., Žvanut, B.: Cross-cultural validation and psychometric testing of the Slovenian version of the Croatian Behavioral-Cognitive Internet Security Questionnaire. ELEKTROTEHNIŠKI VESTNIK **89**(3), 103–108 (2022)
20. Kannelønning, K., Katsikas, S.K.: A systematic literature review of how cybersecurity-related behavior has been assessed. Information and Computer Security **ahead-of-print**(ahead-of-print), (2023) https://doi.org/10.1108/ICS-08-2022-0139
21. McCormac, A., Calic, D., Butavicius, M. A., Parsons, K., Zwaans, T., Pattinson, M. R.: A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses. Australasian Journal of Information Systems **21**, (2017)
22. Kitchenham, B., Pfleeger, S.L.: Principles of survey research part 4: questionnaire evaluation. SIGSOFT Software Engineering Notes **27**(3) 20-–23 (2002)