Higher Education Institutions as Targets for Cyber-attacks: Measuring Employees and Students Cybersecurity Behaviours in the Estonian Academy of Security Sciences

Kate-Riin Kont
Internal Security Department, Estonian Academy of Security Sciences
Tallinn, Estonia
e-mail: kate-riin.kont@sisekaitse.ee

Abstract — **The purpose of this study is to identify the most common characteristics that make users vulnerable, either individually or in groups, and to determine whether there is a relationship between user behaviour and victimisation of a cyber-attack. This research should help characterise people who are more likely to become victims of various phishing and social attacks. For this purpose, students, employees and lecturers of the Estonian Academy of Security Sciences were investigated. A five-scale questionnaire was used as the methodology of the study, which considers the following behaviours: risky behaviour, conservative behaviour, risk exposure behaviour and risk perception behaviour. The results obtained show that users with risky behaviour are most exposed to social engineering attacks in social networks. Furthermore, the analysed groups of faculty and staff fall victim to these attacks less often than students. Finally, we concluded that people who spend more time in front of a computer and engage in riskier cyber behaviours are more vulnerable to attacks.**

Keywords – cyber security, user behaviour, risk, vulnerabilities, higher education institutions, staff, students.

I. Introduction

Across Europe, the number and sophistication of cyber-attacks and cybercrime is increasing. While nearly every major industry faces significant cyber security challenges, higher education is particularly vulnerable for several important reasons.

In particular, it has to do with the unique academic culture, known for its openness and transparency. Criminals can get into the researchers' network and see what is happening, what is being tested, and how those tests are going. Several master's and doctoral theses have taken place in closed defences, with no public access to them, although the university membership or a certain part of it has access. Such data is not only a target for espionage but also has economic value.

Another reason has to do with history – specifically, that higher education institutions have been online for a very long time. Universities have always been the main targets of cyber- attacks because universities have had access to the Internet for a relatively long time. They have always offered free public access, as research centres in their field, not only to their members but also to anyone who wishes, e.g. through their libraries. As a result, they have long been visible targets, and cybercriminals are likely to know their weaknesses very well. A few examples of cyber-attacks on universities show that such an attack can be not only detrimental to relations between countries but even life-threatening.

The University of Helsinki was hit by an exceptionally extensive cyber-attack on 22.03.2022. During the day, up to 2,500 comments were posted on the university's social media accounts from what appeared to be new fake profiles with few posts and followers. The content of the messages was clearly anti-Russian. Among other things, they demanded the withdrawal of the right to study from Russian students. There were 10–15 identical messages, so it could be assumed that it was an automated robot attack. The Russian state was probably behind the attack, and the messages were used to give the university the impression that there are anti-Russian sentiments in Finland or the University of Helsinki. Such attacks could be successfully used, for example, in the Russian media against Finland. Such a large and organised cyber-attack was exceptional at the University of Helsinki [1].

The most serious attacks are those on health care, for example, hospitals. In the Czech Republic, a cyber-attack took place in the middle of March 2020 on a hospital performing corona tests in the city of Brno. The malware locked the hospital's data and demanded a ransom to unlock it [2]. Another example had very serious consequences. Düsseldorf University Hospital failed to admit a woman brought by ambulance on 19.09.2020 after a cyber-attack froze the hospital's information system. The woman later died in the ambulance as it was diverted to another hospital 30km away. As claimed by Reuters, it was the first confirmed case anywhere in the world, in which a person has died as the direct consequence of a cyberattack [3]. However, it was not certain if the university hospital was the actual target of the attack or if it was collateral damage in an attack on the university. The ransom demands were aimed at Heinrich Heine University, not the hospital directly. The police contacted the attackers and informed them that the target of the attack was the hospital, not the university, and that the patient's life was in danger. After that, the attack was stopped and the authorities were given the encryption key, but it was too late [4].

In summary, higher education institutions are targets for cyber-attacks because their data is valuable and easily accessible. In addition to the fact that the personal data of students and staff held by universities presents an opportunity for ransom attacks, the latest research findings could become a target for international espionage. Therefore, it is critical that academic institutions provide resources for cyber security and protect themselves against potential attacks.

The current study examines the behaviour of students, lecturers (researchers) and employees of the Estonian Academy of Security Sciences regarding hybrid threats and possibilities to prevent risks related to cyber security. This study is part of a larger research conducted within the framework of the cooperation program on hybrid threats (HYBRIDC) between Estonian Academy of Security Sciences, Lithuanian Mykolas Romeris University, Academy of Public Security and Riga Stradins University. This questionnaire has been prepared in cooperation with the digital development department of the Estonian Academy of Security Sciences. The results of the study can be used to develop strategies and trainings to reduce errors related to the human factor in the cyber security of higher education institutions. " Th rest of the paper is structured as follows. In Section 2, we give a brief overview of how cyber security awareness among the members of higher education institutions has been studied so far, what have been the conclusions of these studies, and what recommendations have been made in the future. In Section 3 we shortly introduce the research design, methodology used, present the research questions and the course of the study. General results are pesented in Section 4. Finally, we conclude our work in Section 5.

II. LITERATURE REVIEW

Security in a higher education institution is completely different than in the private sector because it is an open institution. There are many access points and a lot of personal information about employees and students. Information security training, awareness raising, and cyber behaviour monitoring are not always top priorities for educational institutions. The contribution of lecturers, researchers and employees who engage in research and teaching work or provide administrative support to these activities are often considered to be the central figures of a higher education institution. Information technology (IT) employees deal with security to the extent that they have the human and time resources for it.

Several studies have shown that there is a human dimension to the causes of cyber-attacks in higher education institutions [5]-[9]. Analysing the data from these studies, it was discovered that the patron's ignorance and carelessness in password management is common, which contributes to higher education institutions becoming targets for cyber-attacks. The studies by Öğütçü et al. [5] and Benavides-Astudillo et al. [9] aimed to identify common characteristics that make users vulnerable to social manipulation, either individually or in groups. For this purpose, they conducted a survey among the employees and students of the higher education institution. Four scales that consider the following behaviours were studied: Risky Behaviour Scale (RBS), Conservative Behaviour Scale (CBS), Exposure to Offence Scale (EOS) and Risk Perception Scale (RPS). Öğütçü et al. [5] results showed that respondents' behaviour becomes more cautious the more they perceive threats. Respondents' use of risky technologies increases their exposure to crime, which in turn increases caution. It also appeared that the score of the group that participated in security training was higher than the score of the group that did not attend such training. This finding clearly shows that such training increases people's awareness. The data analysis showed that the respondents do not report the cybercrime they have experienced to the authorities because they do not know who to turn to. One of the most important findings of this study is that the higher the level of education, the greater their awareness of information security. A notable finding was that students (between the ages of 18 and 30) appear to be the group most at risk [5]. The results of a study conducted by Benavides-Astudillo et al. [9] with the same methodology showed that users with risky behaviour are most exposed to social manipulation attacks in social networks. It also concluded that the analysed faculty and staff groups fall victim to such attacks much less often than students and that people who spend more time online are more likely to fall victim to a social engineering attack [9].

III. RESEARCH METHODOLOGY

To find out the most common reasons that make everyday Internet users, such as students and employees of Estonian higher education institutions, undoubtedly vulnerable, either individually or in groups, the four-scale measure developed by Öğütçü et al. [5] was used. The RBS measures the risk behaviour of Internet users, e.g. whether various security measures are used to protect themselves as well as the people they live or work with. The purpose of the CBS is to measure the Internet user's actions and actions in protecting his personal information. The purpose of the EOS is to measure the exposure of users to any cyber security threat, highlighting the user's behaviour in relation to the risks, threats and effects resulting from the events. The RPS measures the level of risk or threat that befalls the Internet user and is related to the field of trust that the user has in the face of possible cyber-attacks [5], [9].

The scales and questions were developed based on existing literature and IT expert opinions of the Estonian Academy of Security Sciences. It is quite important to determine the level of awareness because awareness and behaviour are very closely related. According to this model, an individual's behaviour is determined by the perception of a threat and actions to resolve that threat. Awareness is a powerful weapon against social engineering attacks, so this study allows universities of applied sciences to use these findings to focus their cyber security training priorities. The survey consists of five parts: 1) questions that collect respondents' demographic data, 2) questions about user profiles related to IT and computer security, 3) questions dealing with risky issues related to IT behaviour, 4) questions about respondents' behaviour regarding information security and threats, and 5) questions that address users' exposure to cybercrime.

Answers could be given according to a 5-point Likert scale. The proposed scales were formulated depending on the questions asked. Total respondent scores were calculated by assigning 5 points for "Always", 4 points for "Often", 3 points for "Sometimes", 2 points for "Rarely", and 1 point for "Never" for the RBS and CBS questions. A higher score indicates that the respondent is very risk tolerant. For EOS, it is said that as the scores increase, the respondent is exposed to crime (negative experience) at a higher level. For RPS, "Very dangerous" is 5 points, "Dangerous" is 4 points, "Slightly dangerous" is 3 points, "Not dangerous" is 2 points and "I don't know" is 1 point. As the scores increase, it is understandable that the respondent considers related technologies more dangerous [5].

Based on the two main studies of RBS, CBS, EOS and RPS [5], [9], the following research questions were raised:

Is there a difference between the scales concerning their average score?

Is there a difference between the surveyed groups (lecturers, administrative staff, and students) concerning their average score?

Does the duration of time spent on the Internet affect the average score of the scales?

Does the cyber security training attendance affect the average score of the scales?

Invitations to participate were sent to the email addresses of 1,000 undergraduate students and 69 master students, 439 faculty members and 271 staff. The survey was conducted using LimeSurvey and was administered by sending a link to the online survey. Data collection lasted for two months, during which repeated reminders were sent. There were 363 total responses including non-completed. The data were screened and any results missing one or more responses were deleted, resulting in a sample size of n=277.

IV. General results

Tables 1 and 2, and Figures 1 and 2 show the results obtained based on the user's general information. Table 1 gives an overview of the demographic data of the users, and here information about the completed/uncompleted cyber training, the time spent on the Internet during the day, as well as the type of Internet access used can be found. Table 2 shows the survey averages for all four defined categories – Risky Behaviour Scale (RBS), Conservative Behaviour Scale – (CBS), Exposure to Offence Scale (EOS) and the Risk Perception Scale (RPS). A score of 1 is considered the lowest value and 5 is the maximum value for each survey question.

TABLE I. Results of the user profile section

Characteristic	Category	Number of respondents	Percentage
Gender	Male	120	43%
	Female	157	57%
Age range	19–25	68	30%
	26–30	27	9%
	31–40	58	19%
	41–50	81	27%
	51–60	32	11%
	61–70	9	3%
	70+	2	1%
Position	Vocational student	33	12%
	Undergraduate student	98	33%
	Graduate student	14	5%
	Lecturers	42	15%
	Administrative staff	71	26%
	Other	19	7%
Cyber security training completed	Yes	241	60%
	No	66	40%
Time spent on the Internet	1–5 hours/day	145	52%
	6–10 hours/day	123	44%
	11 or more hours/day	9	3%
Type of Internet access	Using Mobile Internet	133	48%
	Using public Wi-Fi network (Cafes, shopping centres)	1	1%
	Using private Wi-Fi network (Home)	15	5%
	Using remote connection of my organisation	128	46%

TABLE II. Number of questions and averages obtained by scale

Scale	Number of questions	Average score
RBS	20	2.610469
CBS	10	4.051264
EOS	7	1.38886
RPS	17	3.49777

ISBN: 978-1-68558-113-8

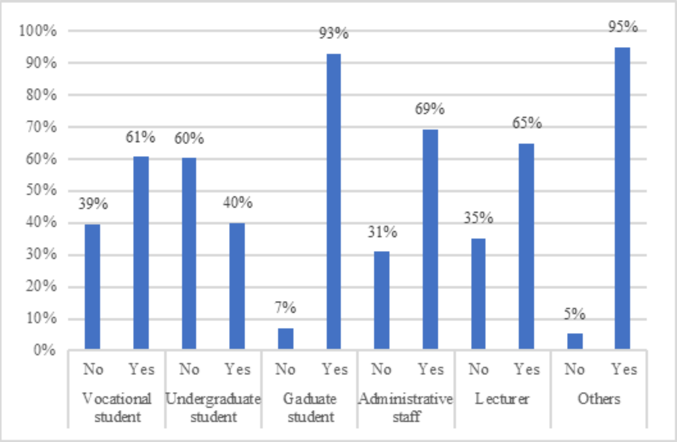

Figure 1. Results of the completed cyber security training

Figure 1 shows that the majority of students who have participated in cyber security training are master's students, and among the employees of the higher education institution, those who have identified themselves as "others", that is, research workers and external lecturers. Notably, 61% of vocational students and only 40% of applied higher education students have completed cyber security training. More than half of the teaching staff and employees have also completed the training. Nonetheless, this level is definitely not high enough.

Figure 2 shows the most eager Internet users in every studied group separately. While undergraduate students and lecturers are the most diligent Internet users in both 1–5 hours/day and 6–10 hours/day groups, the administrative staff is apparently overwhelmed with work in the 11 or more hours/day group.

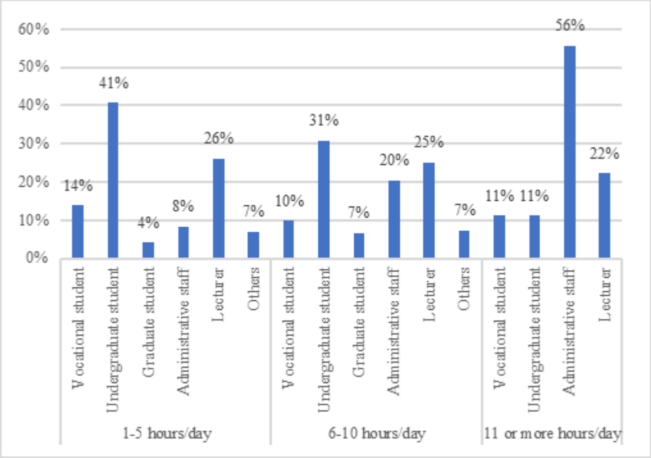

Figure 2. Time range of Internet use according to the position.

V. CONCLUSIONS

It is necessary to emphasise that people's behavior can contribute to making it easier to become victims of cyber-attacks, and it is by raising their awareness that it is possible to mitigate the consequences of cyber-attacks on universities. The model proposed here can be successfully applied to different higher education institutions – it helps quickly find out the cyber security training needs and develop the training policy which can be implemented at the right level of difficulty. Similarly, this model identifies the knowledge and skills of user groups, to deal with social engineering attacks.

REFERENCES

[1] K. Kirsi, "Helsingin yliopisto joutui laajan verkkohyökkäyksen kohteeksi: some-päivityksiin tullut jopa 2 500 venäläisvastaista kommenttia" [in English: "The University of Helsinki was the target of a large-scale online attack: up to 2,500 anti-Russian comments were posted on social media"], YLE News, 2022, March 22. https://yle.fi/a/3-12370984

[2] C. Cimpanu, "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak," ZDNET, 2020, March 13. https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

[3] D. Busvine and T. Kaeckenhoff, "Prosecutors open homicide case after hacker attack on German hospital," Reuters, 2020, September 18. https://www.reuters.com/article/us-germany-cyber-idUSKBN26926X

[4] M. Heikkilä, "Nainen kuoli ambulanssiin, kun kyberhyökkäys jumitti saksalaisen sairaalan tietojärjestelmän – syyttäjä avasi harvinaisen henkirikostutkimuksen," Woman dies in ambulance after cyber-attack freezes German hospital's information system - prosecutor opens rare homicide investigation"], YLE News, 2020, September 19. https://yle.fi/a/3-11553530

[5] G. Öğütçü, Ö. M. Testik and O. Chouseinoglou, "Analysis of personal information security behavior and awareness," Computer & Security, 2016, vol. 56, pp. 83–93. https://doi.org/10.1016/j.cose.2015.10.002

[6] L. Muniandy, B. Muniandy and Z. Samsudi, „Cyber Security Behaviour among Higher Education Students in Malaysia," 2017, Journal of Information Assurance & Cyber Security, 2017, pp. 1-13. DOI: 10.5171/2017.800299

[7] J. Yerby and K. Floyd, "Faculty and Staff Information Security Awareness and Behavior," 2018, Journal of The Colloquium for Information System Security Education (CISSE), vol. 6(1). https://cisse.info/journal/index.php/cisse/article/view/90

[8] Z. Othmana, N. Rahimb and M. Sadiq, "The Human Dimension as the Core Factor in Dealing with Cyberattacks in Higher Education," International Journal of Innovation, Creativity and Change. 2020, vol. 11(1). https://ijicc.net/images/vol11iss1/11101_Othman_2020_E_R.pdf

[9] E. Benavides-Astudillo, L. Silva-Ordoñez, R. Rocohano-Rámos, W. Fuertes, F. Fernández-Peña, S. Sanchez-Gordon and R. Bastidas-Chalan, "Analysis of Vulnerabilities Associated with Social Engineering Attacks Based on User Behavior," in Applied Technologies. ICAT 2021. Communications in Computer and Information Science, vol 1535, M. Botto-Tobar, S. Montes León, P. Torres-Carrión, M. Zambrano Vizuete, B. Durakovic (eds) Springer, Cham. https://doi.org/10.1007/978-3-031-03884-6_26