Survey about cyberattack protection motivation in higher education: Academics at Slovenian universities, 2017

LUKA JELOVČAN, University of Maribor, Slovenia
SIMON VRHOVEC, University of Maribor, Slovenia
ANŽE MIHELIČ, University of Maribor, Slovenia

This paper reports on a study aiming to explore factors associated with motivation of individuals in organizations to protect against cyberattacks. The objectives of this study were to determine how fear of cyberattacks, perceived severity, perceived vulnerability, perceived threats, measure efficacy, self-efficacy, measure costs, mandatoriness and psychological reactance are associated with protection motivation of individuals in organizations. The study employed a cross-sectional research design. A survey was conducted among academics at six Slovenian universities between June and September 2017. A total of 324 respondents completed the survey (7.6 percent response rate) providing for N=255 useful responses after excluding poorly completed responses. The survey questionnaire was developed in English. A Slovenian translation of the survey questionnaire is available.

Additional Key Words and Phrases: PMT, higher education, university, cybersecurity, cyber threat, computer security, internet

1 INTRODUCTION

The survey questionnaire was designed to measure theoretical constructs included in the research model. Most items were taken or adapted from existing literature to fit the study’s context. Table 1 presents the theoretical constructs included in the research model, their definition in this research, and sources from which construct items were taken or adapted.
Table 1. Theoretical constructs in the survey questionnaire.

| Theoretical construct                  | Definition in this research                                                                 | Sources |
|----------------------------------------|---------------------------------------------------------------------------------------------|---------|
| Fear of cyberattacks                   | The level of the individual’s fear of cyberattacks.                                         | [6]     |
| Perceived severity (organization)     | The perceived extent of consequences of a successful cyberattack for the organization.     | [5]     |
| Perceived vulnerability (organization) | The perceived probability of a successful cyberattack on the organization.                   | [5]     |
| Perceived severity (individual)       | The perceived extent of consequences of a successful cyberattack for the individual.        | [5]     |
| Perceived vulnerability (individual)  | The perceived probability of a successful cyberattack on the individual.                    | [5]     |
| Perceived threats                     | The perceived extent of threats to the individual posed by cyberattacks.                    | [5]     |
| Measure efficacy                      | The perceived efficacy of countermeasures against cyberattacks that an individual can implement. | [2]     |
| Self-efficacy                         | The individual’s self-efficacy when implementing countermeasures against cyberattacks.     | [7]     |
| Measure costs                         | The perceived costs of implementing countermeasures against cyberattacks.                  | [9]     |
| Mandatoriness                         | The perceived mandatoriness of implementing countermeasures against cyberattacks.          | [1]     |
| Psychological reactance               | The level of the individual’s motivation toward the reestablishment of threatened or eliminated personal freedoms. | [3]     |
| Protection motivation                 | The level of organizational insider’s motivation to implement countermeasures against cyberattacks. | [4, 8] |

2 METHOD

2.1 Survey instrument

To test the research model, a survey questionnaire was developed. Adapted and new questionnaire items (i.e., fear of cyberattacks, perceived severity (organization), perceived vulnerability (organization), perceived severity (individual), perceived vulnerability (individual), perceived threats, measure efficacy, self-efficacy, measure costs, mandatoriness, psychological reactance, and protection motivation) were developed by following a predefined protocol.

The questionnaire was first developed in English and then translated into Slovenian by two translators independently. The translators developed the Slovenian questionnaire through consensus. The Slovenian questionnaire has been pre-tested by 2 independent respondents who provided feedback on its clarity. Based on the received feedback, the Slovenian questionnaire was reviewed to remove any ambiguity. Items were reworded, added, and deleted in the pre-test. To ensure the consistency between the Slovenian and English questionnaire, the Slovenian questionnaire was translated back to English. No significant differences in the meaning between the original items in English and back-translations were noticed. The English questionnaire was however reviewed to update the items and to remove any ambiguity based on the back-translation.

Table 2 presents the survey questionnaire in English and Table 3 presents the Slovenian translation of the survey questionnaire. All items were measured using a 7-point Likert scale as presented in Table 4.
Table 2. Survey questionnaire items (English original).

| Construct                               | Item                                                                 |
|-----------------------------------------|----------------------------------------------------------------------|
| Perceived threats (PT)                  | PT1. Cyberattacks pose a serious threat to me.                      |
|                                         | PT2. Consequences of successful cyberattacks would highly threaten me.|
|                                         | PT3. Cyberattacks pose a serious danger to me.                      |
| Perceived severity (organization) (PSo)| PSo1. A successful cyberattack on our organization would greatly jeopardize the privacy of its confidential data. |
|                                         | PSo2. A lot of our organization’s confidential data collected by a successful cyberattack could be misused for criminal purposes. |
|                                         | PSo3. A lot of our organization’s confidential data collected by a successful cyberattack could be misused against it. |
| Fear of cyberattacks (FoC)              | FoC1. I am very afraid of cyberattacks.                               |
|                                         | FoC2. The prevalence of cyberattacks is terrifying.                 |
|                                         | FoC3. Potential losses due to cyberattacks are causing me strong discomfort. |
|                                         | FoC4. The danger of cyberattacks is alarming.                       |
| Perceived vulnerability (individual) (PVi)| PVi1. It is very likely that I will be a victim of a cyberattack in the future. |
|                                         | PVi2. My chances of becoming a victim of a cyberattack are very high.|
|                                         | PVi3. I strongly feel that I will become a victim of a cyberattack in the future. |
| Perceived severity (individual) (PSi)   | PSi1. A successful cyberattack would greatly jeopardize my privacy.  |
|                                         | PSi2. A lot of my personal data collected by a successful cyberattack could be misused for criminal purposes. |
|                                         | PSi3. A lot of my personal data collected by a successful cyberattack could be misused against me. |
| Perceived vulnerability (organization) (PVo)| PVo1. It is very likely that our organization will become a victim of a cyberattack in the future. |
|                                         | PVo2. Chances of our organization becoming a victim of a cyberattack are very high. |
|                                         | PVo3. I strongly feel that our organization will become a victim of a cyberattack in the future. |
| Mandatoriness (M)                       | M1. I am required to take protective measures against cyberattacks according to the organization’s information security policy. |
|                                         | M2. It is expected that I play an active role in taking protective measures against cyberattacks. |
|                                         | M3. It is expected that I strictly adhere to organizational information security policies and procedures for protecting against cyberattacks. |
| Psychological reactance (PR)            | PR1. When something is prohibited, I usually think: ‘That’s exactly what I am going to do.’ |
|                                         | PR2. I consider advice from others as an intrusion.                 |
|                                         | PR3. Advice and recommendations induce me to do just the opposite.   |
|                                         | PR4. I resist attempts of others to influence my decisions.          |
|                                         | PR5. Organizational rules regarding the use of protective measures against cyberattacks trigger a sense of resistance in me. |
|                                         | PR6. I become annoyed when I am not able to make free and independent decisions about protective measures against cyberattacks. |
|                                         | PR7. I become angry if my freedom of choice regarding protective measures against cyberattacks is restricted. |
|                                         | PR8. When someone is forcing me to take protective measures against cyberattacks, I feel like doing the opposite. |
| Measure efficacy (ME)                   | ME1. The success rate of protective measures against cyberattacks is very high. |
|                                         | ME2. The probability of stopping cyberattacks by taking protective measures is very high. |
|                                         | ME3. The likelihood of neutralizing cyberattacks by taking protective measures is very high. |
| Self-efficacy (SE)                      | SE1. I have no problems using protective measures against cyberattacks. |
|                                         | SE2. Taking a protective measure against cyberattacks is entirely under my control. |
|                                         | SE3. I have all resources and skills needed to take protective measures against cyberattacks. |
| Measure costs (MC)                      | MC1. Taking protective measures against cyberattacks is very work-intensive. |
|                                         | MC2. Taking protective measures against cyberattacks requires a lot of effort. |
|                                         | MC3. Taking protective measures against cyberattacks is very time-consuming. |
| Protection motivation (PM)              | PM1. I intend to take protective measures against cyberattacks in the future. |
|                                         | PM2. I predict that I will take protective measures against cyberattacks in the future. |
|                                         | PM3. I plan to take protective measures against cyberattacks in the future. |
| Construct | Item |
|-----------|------|
| Perceived threats (PT) | PT1. Spletni napadi mi predstavljajo resno grožnjo. |
| | PT2. Posledice uspešnih spletnih napadov bi me močno ogrozile. |
| | PT3. Spletni napadi mi predstavljajo resno nevarnost. |
| Perceived severity (organization) (PSo) | PSo1. Uspešen spletni napad bi zelo ogrozil zasebnost zaupnih podatkov naše organizacije. |
| | PSo2. Ob uspešnem spletnem napadu bi bilo veliko zaupnih podatkov naše organizacije lahko zlorabljenih v kriminalne namene. |
| | PSo3. Ob uspešnem spletnem napadu bi bilo lahko veliko zaupnih podatkov naše organizacije zlorabljenih zoper našo organizacijo. |
| Fear of cyberattacks (FoC) | FoC1. Zelo se bojim spletnih napadov. |
| | FoC2. Razširjenost spletnih napadov je zastrašujoča. |
| | FoC3. Potencialne izgube zaradi spletnih napadov v meni zbujojo močno neprijetnost. |
| | FoC4. Nevarnost spletnih napadov je zaskrbljujoča. |
| Perceived vulnerability (individual) (PVi) | PVi1. V prihodnosti bom zelo verjetno žrtev spletnega napada. |
| | PVi2. Obstaja velika verjetnost, da postanem žrtev spletnega napada. |
| | PVi3. Močno se mi zdi, da bom v prihodnosti postal žrtev spletnega napada. |
| Perceived severity (individual) (PSi) | PSi1. Uspešen spletni napad bi zelo ogrozil mojo zasebnost. |
| | PSi2. Ob uspešnem spletnem napadu bi bilo veliko mojih osebnih podatkov zlorabljenih v kriminalne namene. |
| | PSi3. Ob uspešnem spletnem napadu bi bilo lahko veliko mojih osebnih podatkov zlorabljenih zoper mene. |
| Perceived vulnerability (organization) (PVo) | PVo1. Naša organizacija bo v prihodnosti zelo verjetno žrtev spletnega napada. |
| | PVo2. Obstaja velika verjetnost, da naša organizacija postane žrtev spletnega napada. |
| | PVo3. Močno se mi zdi, da bo naša organizacija v prihodnosti postala žrtev spletnega napada. |
| Mandatoriness (M) | M1. Od mene se zahteva uporaba zaščitnih ukrepov proti spletnim napadom v skladu z informacijsko-varnostno politiko organizacije. |
| | M2. Od mene se prizakaja igranje aktivne vloge pri uporabi zaščitnih ukrepov proti spletnim napadom. |
| | M3. Od mene se prikazuje poskusno oznanjavo in razumijevanje organizacijske informacijsko-varnostne politike in postopkov za svojo integriteto v spletnih napadih. |
| Psychological reactance (PR) | PR1. Če je nekaj prepovedano, si navadno mislim: “Točno to bom naredil.” |
| | PR2. Nasvet ostalih dojemam kot vsiljevanje. |
| | PR3. Nasveti in predlogi v meni sprožijo željo, da se soočajem z nekaterimi izgube. |
| | PR4. Upram se poskusom, da bi drugi vplivali name in na moje odlukovanje. |
| | PR5. Organizacijska pravila o uporabi zaščitnih ukrepov proti spletnim napadom v meni sprožijo občutek odpora. |
| | PR6. Če ne morem svobodno in neudaješno odločati o zaščitnih ukrepih proti spletnim napadom, postanem nevoljen. |
| | PR7. Omejevanje moje svobode odločanja o zaščitnih ukrepih proti spletnim napadom me ujedi. |
| Measure efficacy (ME) | ME1. Zaščitni ukrepi proti spletnim napadom so lahko resno uspešni. |
| | ME2. Zaščitni ukrepi proti spletnim napadom so lahko zelo uspešni. |
| | ME3. Zaščitni ukrepi proti spletnim napadom so lahko zelo uspešni. |
| | ME4. Zaščitni ukrepi proti spletnim napadom so lahko zelo uspešni. |
| | ME5. Zaščitni ukrepi proti spletnim napadom so lahko zelo uspešni. |
| | ME6. Zaščitni ukrepi proti spletnim napadom so lahko zelo uspešni. |
| | ME7. Zaščitni ukrepi proti spletnim napadom so lahko zelo uspešni. |
| | ME8. Zaščitni ukrepi proti spletnim napadom so lahko zelo uspešni. |
| Self-efficacy (SE) | SE1. Nimam težav pri uporabi zaščitnih ukrepov proti spletnim napadom. |
| | SE2. Upram se soočajem z težavami pri uporabi zaščitnih ukrepov proti spletnim napadom. |
| | SE3. Imam vsa potrebna sredstva in znanje za uporabo zaščitnih ukrepov proti spletnim napadom. |
| Measure costs (MC) | MC1. Uporaba zaščitnih ukrepov proti spletnim napadom zahteva veliko delo. |
| | MC2. Uporaba zaščitnih ukrepov proti spletnim napadom zahteva veliko truda. |
| | MC3. Uporaba zaščitnih ukrepov proti spletnim napadom je zelo zamudna. |
| Protection motivation (PM) | PM1. V prihodnosti namenjavam uporabljati zaščitne ukrepe proti spletnim napadom. |
| | PM2. Predvidevam, da bom v prihodnosti uporabljal zaščitne ukrepe proti spletnim napadom. |
| | PM3. Načrtujem uporabo zaščitnih ukrepov proti spletnim napadom v prihodnosti. |
Table 4. 7-point Likert scale.

| Score | English          | Slovenian                  |
|-------|------------------|----------------------------|
| 1     | Strongly disagree| Močno se ne strinjam       |
| 2     | Disagree         | Se ne strinjam             |
| 3     | Somewhat disagree| Delno se ne strinjam       |
| 4     | Neutral          | Nevtralno                  |
| 5     | Somewhat agree   | Delno se strinjam          |
| 6     | Agree            | Se strinjam                |
| 7     | Strongly agree   | Močno se strinjam          |

2.2 Data collection

We conducted the survey with the Slovenian translation of the questionnaire among academics at six Slovenian universities between 13 June 2017 and 3 September 2017. Respondents were recruited through e-mail addresses which were publicly available at the official websites of universities and their departments. The respondents did not receive any compensation for taking the survey. A total of 4,291 e-mails were sent, and 324 respondents completed the survey providing for a response rate of 7.6 percent. After excluding poorly completed responses (responses with over 50 percent of missing values or standard deviation equal to 0 for constructs fear of cyberattacks, perceived severity (organization), perceived vulnerability (organization), perceived severity (individual), perceived vulnerability (individual), perceived threats, measure efficacy, self-efficacy, measure costs, mandatoriness, psychological reactance and protection motivation), we were left with 255 useful responses as presented in Table 5.

The first page of the survey is presented in Table 6.
Table 5. Sample with the number of sent invitations, number of responses, and number of useful responses (N) after excluding poorly completed responses.

| ID | Name          | Sent invitations | Responses | N  |
|----|---------------|------------------|-----------|----|
| 1  | UL AGRFT      | 37               | 2         | 1  |
| 2  | UL BF         | 564              | 31        | 26 |
| 3  | UL EF         | 127              | 6         | 6  |
| 4  | UL FA         | 55               | 2         | 2  |
| 5  | UL FDV        | 165              | 11        | 10 |
| 6  | UL FE         | 118              | 11        | 5  |
| 7  | UL FGG        | 199              | 16        | 14 |
| 8  | UL FKKT       | 180              | 11        | 6  |
| 9  | UL FMF        | 181              | 11        | 6  |
| 10 | UL FPP        | 84               | 5         | 4  |
| 11 | UL FRI        | 121              | 3         | 3  |
| 12 | UL FS         | 126              | 8         | 6  |
| 13 | UL FSD        | 26               | 7         | 6  |
| 14 | UL FŠP        | 91               | 7         | 5  |
| 15 | UL NTF        | 91               | 9         | 8  |
| 16 | UL PEF        | 148              | 14        | 13 |
| 17 | UL PF         | 41               | 2         | 2  |
| 18 | UL TEOF       | 45               | 5         | 4  |
| 19 | UL ZF         | 94               | 10        | 10 |
| 20 | UM EPF        | 69               | 2         | 1  |
| 21 | UM FE         | 30               | 2         | 2  |
| 22 | UM FERI       | 276              | 26        | 17 |
| 23 | UM FF         | 105              | 5         | 3  |
| 24 | UM FKBV       | 65               | 1         | 1  |
| 25 | UM FKKT       | 38               | 0         | 0  |
| 26 | UM FL         | 26               | 2         | 1  |
| 27 | UM FNM        | 78               | 8         | 6  |
| 28 | UM FS         | 189              | 26        | 20 |
| 29 | UM FT         | 33               | 4         | 3  |
| 30 | UM FVV        | 24               | 7         | 7  |
| 31 | UM FŽV        | 34               | 6         | 3  |
| 32 | UM MF         | 46               | 1         | 0  |
| 33 | UM PEF        | 71               | 4         | 4  |
| 34 | UM PF         | 39               | 0         | 0  |
| 35 | UNG FH        | 43               | 3         | 3  |
| 36 | UNG FN        | 13               | 0         | 0  |
| 37 | UNG FŽO       | 35               | 1         | 1  |
| 38 | UNG PTF       | 18               | 1         | 1  |
| 39 | UNG VŠVV      | 18               | 1         | 0  |
| 40 | UNM FII       | 27               | 2         | 2  |
| 41 | UNM FIŠ       | 31               | 6         | 6  |
| 42 | UNM FOŠ       | 30               | 6         | 6  |
| 43 | UPR FAMNIT    | 159              | 8         | 4  |
| 44 | UPR FIŠŠ      | 62               | 0         | 0  |
| 45 | UPR FM        | 64               | 7         | 4  |
| 46 | UPR FTŠŠ      | 39               | 6         | 5  |
| 47 | UPR PEF       | 103              | 13        | 13 |
| 48 | VSNM FPUV     | 9                | 0         | 0  |
| 49 | VSNM FTS      | 5                | 0         | 0  |
| 50 | VSNM FUPI     | 12               | 2         | 2  |
| 51 | VSNM FŽV      | 7                | 3         | 3  |

Total 4,291 324 255
Dear Sirs,

We invite you to participate in a study on self-protection against cyberattacks which is carried out by the Faculty of Security Sciences at the University of Maribor. This study aims to gain an insight into the factors that influence the decisions of employees to take measures to protect against malicious software. Estimated time to complete the survey is 4-5 minutes.

For additional information regarding the study, contact us at simon.vrhovec@fvv.uni-mb.si.

---

Table 6. The first page of the survey.

| English original | Slovenian translation |
|------------------|-----------------------|
| Self-protection of employees against cyberattacks | Samovarovanje zaposlenih pred spletnimi napadi |
| Dear Sirs, | Spojstovani, |
| We invite you to participate in a study on self-protection against cyberattacks which is carried out by the Faculty of Security Sciences at the University of Maribor. This study aims to gain an insight into the factors that influence the decisions of employees to take measures to protect against malicious software. Estimated time to complete the survey is 4-5 minutes. | vabimo vas k sodelovanju v raziskavi o samovarovanju pred spletnimi napadi, ki jo izvajamo na Fakulteti za varnostne vede Univerze v Mariboru. Z raziskavo želimo pridobiti vpogled v dejavnike, ki vplivajo na odločitve zaposlenih o sprejemjanju ukrepov za zaščito pred škodljivo programsko opremo. Predviden čas izpolnjevanja ankete je 4-5 minut. |
| For additional information regarding the study, contact us at simon.vrhovec@fvv.uni-mb.si. | Za dodatne informacije v zvezi z raziskavo nam pišite na simon.vrhovec@fvv.uni-mb.si. |

3 RESULTS

3.1 Sample

Demographic characteristics of the sample are presented in Table 7.

Table 7. Demographic characteristics of the sample.

| Characteristic       | Value      | Frequency |
|----------------------|------------|-----------|
| Gender               | 1 – Male   | 106       |
|                      | 2 – Female | 134       |
|                      | Missing    | 84        |
| Age group            | 21-25      | 8         |
|                      | 26-30      | 26        |
|                      | 31-35      | 36        |
|                      | 36-40      | 29        |
|                      | 41-45      | 42        |
|                      | 46-50      | 24        |
|                      | 51-55      | 30        |
|                      | 56-60      | 16        |
|                      | 61-65      | 20        |
|                      | 66-70      | 5         |
|                      | 71 or more | 5         |
|                      | Missing    | 83        |
| Formal education     | High school or less | 4 |
|                      | Bachelor’s degree | 7 |
|                      | Master’s degree | 64 |
|                      | PhD degree   | 163       |
|                      | Missing      | 86        |
3.2 Frequencies

Frequencies of all variables for measured theoretical constructs are presented in Table 8.

| Variable  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | Valid | Missing | Total |
|-----------|---|---|---|---|---|---|---|-------|---------|-------|
| PT1       | 8 | 31|19 |26 | 81|106|48 |319   | 5       | 324   |
| PT2       | 3 | 30|18 |26 | 71|102|67 |317   | 7       | 324   |
| PT3       | 7 | 35|19 |24 | 83|102|47 |317   | 7       | 324   |
| PSo1      | 6 | 10|14 |25 | 51|94 |109|309   | 15      | 324   |
| PSo2      | 15| 53|24 |38 | 70|60 |42 |302   | 22      | 324   |
| PSo3      | 13| 44|25 |34 | 84|61 |41 |302   | 22      | 324   |
| FoC1      | 13| 56|30 |46 | 81|48 |19 |293   | 31      | 324   |
| FoC2      | 9 | 30|26 |45 | 54|83 |43 |290   | 34      | 324   |
| FoC3      | 12| 51|30 |43 | 67|58 |30 |291   | 33      | 324   |
| FoC4      | 6 | 18|19 |26 | 73|100|48 |290   | 34      | 324   |
| PVi1      | 23| 52|33 |62 | 51|31 | 3 |255   | 69      | 324   |
| PVi2      | 19| 60|33 |57 | 47|40 | 5 |261   | 63      | 324   |
| PVi3      | 23| 73|31 |63 | 42|23 | 5 |260   | 64      | 324   |
| PSi1      | 10| 45|33 |34 | 73|56 |21 |272   | 52      | 324   |
| PSi2      | 21| 65|35 |45 | 56|35 |10 |267   | 57      | 324   |
| PSi3      | 21| 57|33 |43 | 68|37 |10 |269   | 55      | 324   |
| PVo1      | 8 | 34|26 |61 | 55|39 |12 |235   | 89      | 324   |
| PVo2      | 6 | 34|29 |58 | 46|42 |19 |234   | 90      | 324   |
| PVo3      | 8 | 44|32 |57 | 52|31 |11 |235   | 89      | 324   |
| M1        | 7 | 23|11 |33 | 42|81 |51 |248   | 76      | 324   |
| M2        | 10| 28|20 |37 | 51|69 |32 |247   | 77      | 324   |
| M3        | 5 | 17|14 |30 | 51|67 |65 |249   | 75      | 324   |
| PR1       | 114|99 | 4 |14 | 7 |4  |3  |245   | 79      | 324   |
| PR2       | 66| 135|16 |13 |10 |1  |2  |243   | 81      | 324   |
| PR3       | 91| 122|12 |10 | 6 |1  |2  |244   | 80      | 324   |
| PR4       | 32| 73 |36 |47 | 19|26 |11 |244   | 80      | 324   |
| PR5       | 61|116 |17 |30 | 10| 5 | 4 |243   | 81      | 324   |
| PR6       | 56|114 |19 |22 | 17|10 |4  |242   | 82      | 324   |
| PR7       | 62|117 |15 |22 | 12|12 |3  |243   | 81      | 324   |
| PR8       | 100|110 |8 |14 | 4 |3  |2  |241   | 83      | 324   |
| ME1       | 2 | 4 | 4 |13 | 50|120|36 |229   | 95      | 324   |
| ME2       | 1 | 6 | 6 |17 | 61|102|35 |228   | 96      | 324   |
| ME3       | 2 | 7 | 8 |21 | 61|101|27 |227   | 97      | 324   |
| SE1       | 3 | 4 |11 |21 | 28|111|53 |231   | 93      | 324   |
| SE2       | 7 | 20|17 |53 | 72|50 |10 |229   | 95      | 324   |
| SE3       | 15| 45|31 |36 | 60|40 | 7 |234   | 90      | 324   |
| MC1       | 5 | 34|23 |40 | 58|45 |11 |216   | 108     | 324   |
| MC2       | 4 | 34|27 |39 | 55|45 |11 |215   | 109     | 324   |
| MC3       | 9 | 39|30 |48 | 48|36 | 7 |217   | 107     | 324   |
| PM1       | 3 | 3 | 3 |25 | 44|110|40 |226   | 98      | 324   |
| PM2       | 2 | 3 | 2 |21 | 36|118|47 |229   | 95      | 324   |
| PM3       | 7 | 7 |12 |45 | 51|91 |31 |224   | 100     | 324   |
**4 DISCUSSION**

This paper presents the results of a survey about cyberattack protection motivation in higher education. Future studies may focus on other factors associated with protection motivation of individuals in organizations. Such studies would be beneficial both to better explain protection motivation of organizational insiders, and to better understand the associations between different factors associated with it.

**ACKNOWLEDGEMENTS**

We would like to express our sincere gratitude to the respondents who took their time to participate in our survey.

**REFERENCES**

[1] Scott R. Boss, Laurie J. Kirsch, Ingo Angermeier, Raymond A. Shingler, and R. Wayne Boss. 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems* 18, 2 (2009), 151–164. https://doi.org/10.1057/ejis.2009.8

[2] Yan Chen and Fatemeh Mariam Zahedi. 2016. Individuals’ Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly* 40, 1 (2016), 205–222. https://doi.org/10.25300/MISQ/2016.40.1.09

[3] Sung-Mook Hong and Sandra Page. 1989. A Psychological Reactance Scale: Development, Factor Structure and Reliability. *Psychological Reports* 64, 3_suppl (1989), 1323–1326. https://doi.org/10.2466/prt.1989.64.3c.1323

[4] Jurjen Jansen and Paul van Schaik. 2018. Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior* 87 (2018), 371–383. https://doi.org/10.1016/j.chb.2018.05.010

[5] Huigang Liang and Yajiong Xue. 2010. Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems* 11, 7 (2010), 394–413.

[6] Augustine Osman, Francisco X. Barrios, Joylene R. Osman, Raelynn Schneekloth, and Josh A. Troutman. 1994. The Pain Anxiety Symptoms Scale: Psychometric properties in a community sample. *Journal of Behavioral Medicine* 17, 5 (1994), 511–522. https://doi.org/10.1007/BF01857923

[7] Shirley Taylor and Peter A. Todd. 1995. Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research* 6, 2 (1995), 144–176. https://doi.org/10.1287/isre.6.2.144

[8] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly* 27, 3 (2003), 425–478. https://doi.org/10.2307/30036540

[9] I. M. Y. Woon, G. W. Tan, and R. T. Low. 2005. A Protection Motivation Theory Approach To Home Wireless Security. In *ICIS 2005 Proceedings*. Association for Information Systems, Las Vegas, NV, US, 367–380.