# Risk Assessment Factors, Anxiety, and Cyber-incident Experiences of Cybersecurity Students

Emre Tokgoz, Joel Joseph, Tanvir Ahmed, Julissa Molina, Sergio Duarte, Alyssa Xiang
State University of New York, Farmingdale, NY, tokgoze, josej18, ahmet9, molij17, duarsp, xiana21 @farmingdale.edu

*Abstract* – **Ability of cybersecurity students to assess risk is an important ability expected in the profession. Several different factors impact cybersecurity students' ability to learn such concepts. In addition, cyber-incidents experienced by the students may also have a role in their choices of cybersecurity. Finally, anxiety also plays a role in their learning. Given these considerations, we collected relevant data based on three research questions from 101 students upon Institutional Review Board (IRB) approval at a university located in the Northeast side of the United States. Qualitative and quantitative data are collected for a comprehensive analysis of the data from the research participants (RPs). The quantitative analysis included statistical analysis, best mathematical model fitting, cross-correlation with heatmap evaluation, and Mann-Whitney U- and Kruskal-Wallis H-tests. The qualitative analysis relied on the transcribed information from the video recorded responses as a follow-up to the RPs' answers to the research questions; Money compensation is provided to the RPs for participating in the video recorded interviews. The overall analysis indicated the impact of RPs real-life experiences, professor's examples and explanations in the classroom, RPs' practice of the theory in real life, and the professor's ability to explain the theory for risk assessment. Approximately 94% of the RPs happened to either self-experienced or someone around them (either in the family or friends) experienced a cyber-incident. Finally, about 87% of the participants have some sort of anxiety on occasions. The qualitative results agreed with the quantitative results that will be demonstrated with examples in this work.**

*Index Terms*-Cybersecurity undergraduate student education; Cybersecurity students' worry levels towards success; Factors impacting cybersecurity students' success; Pedagogical cybersecurity research.

## INTRODUCTION

Risk assessment is a vital skill for anyone wishing to enter the cybersecurity profession. It allows identification of vulnerabilities, forecast potential threats and implement preventive measures. As cybersecurity develops in the face of new technologies and increasing sophistication of threats, the need for well-preparedness for having good risk assessment skills is always important in the field of cybersecurity. In alignment with this important concept, our aim in this study is to investigate how educational strategies, personal experiences and psychological factors combine to enable students to develop the necessary skills to assess risks in the cybersecurity environment effectively from a pedagogical perspective. Developing and evaluating cybersecurity competencies for students in computing programs is vital in the general cybersecurity framework [3]. To the best of our knowledge, there are no research literature articles on educating cybersecurity students on risk assessment. One somehow relevant research is related to enhancing students' learning in cybersecurity education using an out-of-class learning approach that can be useful when it comes to improving overall educational outcomes [4]. One of the non-pedagogical studies that is also somehow relevant to our study investigates how often students are careful or conscious of the security of the information they enter in different learning environments [1]. Another such study is [5] that supports the idea of including cybersecurity content in the IT curriculum to better prepare students for the real world; The authors of the study discovered the inclusion of relevant cybersecurity content in an existing curriculum to improve students' knowledge and practice of cybersecurity. It is also important to develop proper risk assessment strategies to implement the best cybersecurity risk management approach that involves technological and education-based solutions, to safeguard systems [2]. Apart from the educational factors, personal and vicarious experiences with cybersecurity incidents are observed to be very useful. In addition, psychological factors such as anxiety and motivation cannot be ignored as a part of the learning experiences of the students; hence, examining the impact of psychological and emotional factors on learning is crucial [6]. In this research, our aim is to empirically investigate the responses of undergraduate cybersecurity students to the following research questions:

1. Which of the following factors do cybersecurity students believe impact their ability to assess risk in cybersecurity?
   - Statistics knowledge
   - Knowledge of the theoretical contents from the courses
   - Practice of the theory on real life risk assessment applications
   - Real-life experiences of the student in risk assessment
   - Professors' examples and explanations
   - Courses
   - Lectures

- Professors' ability to explain.

2. Did the learner or anyone around the learner happen to experience any key personal experiences (such as, encountering a cybersecurity breach, online privacy concerns, or participation in tech programs) in the past that played a role in shaping your interest in a cybersecurity field?
3. Student's anxiety levels impact learning

The following section covers the methodology followed for collecting and analyzing the research data. The third section focuses on the quantitative results derived from the statistical analysis of the collected data from the participants based on their answers to the research questions. The fourth section contains the qualitative analysis results gathered from the research participants based on the video interviews conducted by the Principal Investigator (PI). Conclusions and future work are summarized in the last section to outline the study and the attained results.

## RESEARCH METHODOLOGY

The data depicted in this research was conducted in one of the public universities in the Northeastern region of the United States by the PI and five research assistants. The data is gathered by the research team by following the Institutional Review Board (IRB) approved guidelines. Pre- and post-data collection and evaluation consisted of two informed consent forms, a survey, and video recordings of the interview participants with the transcription of the data. All data is gathered from cybersecurity students. The quantitative data is the numerical data attained from 103 students based on the three research questions outlined in the previous section. The quantitative analysis relied on the Mann-Whitney U-test and the Kruskal-Wallis H-test to identify significant trends and correlations in the responses of participants using statistical methods. Heatmaps were also generated to visualize the relationship between different influencing factors. Additional distributions of the data patterns are evaluated as a part of the quantitative analysis. Follow up interviews were conducted after collecting research question data to qualitatively analyze the data with the aim of gaining deeper understanding of the preliminary responses. These interviews were transcribed and analyzed thematically to identify the nuances of the participants' experiences. Research participants are compensated with money for their participation in the research. Thus, integrated quantitative and qualitative results are carried out to further understand the pedagogical needs of cybersecurity students and help educators to have a better insight into the learners' educational needs. The results can be useful for educators and program developers to know what to include in cybersecurity education.

## QUANTITATIVE RESULTS

The initial data collected from the research participants (RPs) were in the numerical form that allows the application of statistical analysis. The ability to assess risk in cybersecurity is important and the quantitative analysis we present in this section forms the basis on RPs' views of the factors that impact them the most. In addition, we present numerical analysis on experiences of RPs' cybersecurity incidents as well as the impact of anxiety on their education. The techniques we utilize in this section for statistical analysis after cleaning the data include the following:

- Statistical data distribution equation
- Mann-Whitney test
- Kruskal-Wallis Test
- Correlation analysis
- Heatmap of cross-correlations

The results attained in this section will be integrated into qualitative results for attaining stronger results with more comprehensive explanations of the participants in this work.

### *I. Statistical Data Distribution & Correlation Analysis*

Given the limited investment in pedagogical cybersecurity research, the assessment of undergraduate students' beliefs in their cybersecurity risk assessment has not been investigated in the pedagogical research literature to the best of our knowledge. In addition, the impact of cyber-events experienced by the undergraduate students of their relatives or friends might be impacting their educational and career choices, therefore we also investigate such experiences of the RPs. The last part of our investigation is related to the anxiety levels of students impacting their learning. Therefore, the following three parts related to the three questions we investigate are analyzed in this work.

**Part A.** Possible factors that the students believe impacting their ability to assess risk in cybersecurity:

- Student's statistics knowledge
- Student's knowledge of the theoretical contents from the courses
- Student's practice of the theory on real life risk assessment applications
- Student's real-life experiences in risk assessment
- Professor's examples and explanations
- Courses
- Lectures
- Professor's ability to explain.

**Part B.** Research participant's (RP's) or anyone close to this person happens to experience any key personal experiences (such as, encountering a cybersecurity breach, online privacy concerns, or participation in tech programs) in the past that played a role in shaping the RP's interest in a cybersecurity field.

- RP personally experienced
- RP's family members experienced.

- At least one of RP's friends experienced it.

**Part C.** RP's anxiety levels impact self-learning.

The responses to Part A of the research are displayed in Figure I below. A linear regression model is determined to be a good fit to the cleaned data due to the $R^2$ value of 92.92%. Among the options chosen by the participants, the top placement is shared by students' real-life experiences as well as professor's examples and explanations in the classroom that are both rated by 15.46% of the RPs. The top second choice was RPs belief of the ability to practice the theory in real life that was favored by 15.12% of the RPs. The professor's ability to explain the theory got the third placement with a rate of 13.75%.

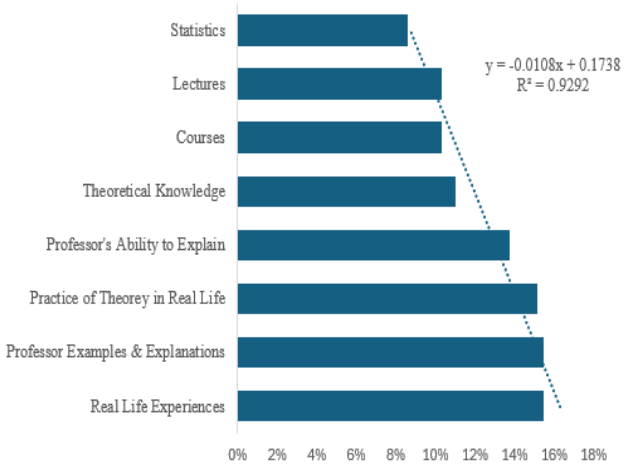


FIGURE I
STATISTICAL DATA DISTRIBUTION OF PARTICIPANTS' PART A CHOICES

The cyber-incident experiences of the students can have an impact on their career choices as well as success in their majors. As an attempt to further understand and analyze undergraduate cybersecurity students, their family members, or friends' experiences, we asked the participants if they had any such challenges or issues. Only 5.71% of the participants did not respond to this part of the question by leaving it blank while the remaining participants are demonstrated in Figure II below as the analysis of Part B responses. The top choice turned out to be 40% of the RPs personally experiencing such an event while the second choice was friend(s) of RPs experiencing such an event at a rate of 34%. The last option was determined to be 26% of RPs' family participants experiencing such an event. The details of the responses to this section will be covered in the qualitative analysis section.

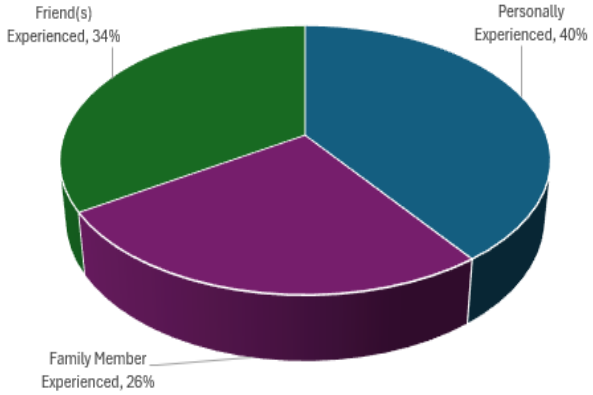


FIGURE II
CYBER-INCIDENT EXPERIENCES OF RPS

The third and last part of the data collection focused on the anxiety and its impact on the RP's learning that formed the Part C portion of the data. The top choice of "Sometimes" was favored by 44% of the RPs while the second choice of "Yes" was favorable at a rate of 43% as a close-cut value to the top choice. Only 13% of the participants claimed that their anxiety does not impact their learning. The details of the responses to this section will also be covered in the qualitative analysis section.

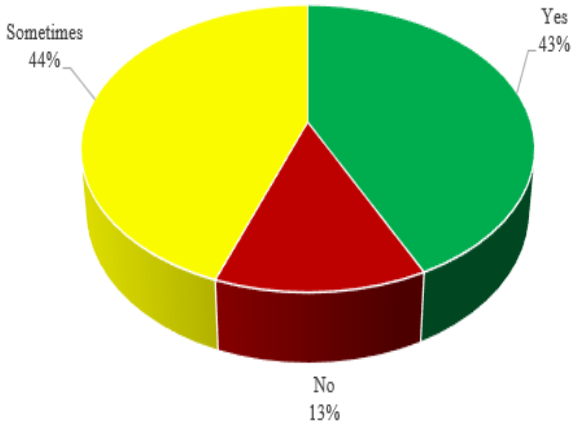


FIGURE III
IMPACT OF ANXIETY ON CYBERSECURITY STUDENTS LEARNING

*II. Cross Correlation Analysis by Using Heatmap*

In this section we evaluate possible cross-correlations on the attained data. The cross-correlation of options for Part A is an indicator of the overlap of the choices made by the RPs for this part that results in coupled correlation analysis for the entire data set attained for Part A; Such a heatmap is designed for Part A that is illustrated in Figure 2 below. The organization of the heatmap is driven by the number of choices made for each column that is made up of the choices and this results in an asymmetric structure of the cross correlations between variables. To illustrate an example, the cross section of the "Statistics" column and "Theoretical Knowledge" column has 68% correlation value with respect

to the number of "Statistics" selections indicating that the RPs who believed knowledge of statistics is important also selected the importance of theoretical knowledge with respect to the number of statistics selections. To the contrary of this, among those who believe that theoretical knowledge is important, only 53.13% of them also believed statistical knowledge is essential for risk assessment abilities.

Analyzing the data in Figure IV in its entirety, statistics (row) had the lowest correlation with all column options indicating that those participants who believed all options other than statistics had the least correlation with the statistics option selection. The second least favored option in correlation to all others was the theoretical knowledge based on the heatmap data. The top two selections that had the highest correlation with all other options were students' practice of theory in real life and professors' examples and explanations.

| | Statistics | Theoretical Knowledge | Practice of Theorey in Real Life | Real Life Experiences | Professor Examples & Explanations | Courses | Lectures | Professor's Ability to Explain |
|---|---|---|---|---|---|---|---|---|
| Statistics | | 53.13% | 43.18% | 37.78% | 33.33% | 50% | 50% | 40% |
| Theoretical Knowledge | 68% | | 59% | 53.33% | 48.89% | 73.33% | 66.67% | 52.50% |
| Practice of Theorey in Real Life | 76% | 81.25% | | 77.78% | 62.22% | 67% | 66.67% | 62.50% |
| Real Life Experiences | 68% | 75% | 79.55% | | 62.22% | 60.00% | 56.67% | 60.00% |
| Professor Examples & Explanations | 60% | 68.75% | 63.64% | 62.22% | | 83.33% | 76.67% | 77.50% |
| Courses | 60% | 68.75% | 45.45% | 40% | 55.56% | | 73.33% | 60.00% |
| Lectures | 60% | 62.50% | 45.45% | 38% | 51.11% | 73.33% | | 65.00% |
| Professor's Ability to Explain | 64% | 65.63% | 56.82% | 53% | 68.89% | 80.00% | 86.67% | |

FIGURE IV
HEAT MAP OF PART A'S CHOICES CROSS-CORRELATIONS

A distribution fit to the averages of the cross-correlation values attained for Figure IV is demonstrated in Figure V. This linear regression is a strong fit to the data based on $R^2$=95.72%. The values used for this figure are displayed in Table I that also includes the associated standard deviations based on column averages of the data attained for Part A. The "Courses" and "Lectures" options selected by the participants had the highest top two averages of 69.52% and 68.1%, respectively. The third option was the students' theoretical knowledge with an average of 67.86%. The lowest average is attained for real life experiences of the students with an average of 51.75%. Hence, for instance, within the category of the participants that selected the "Courses" option, there is an average of 69.52% overlap of selections with the other options.

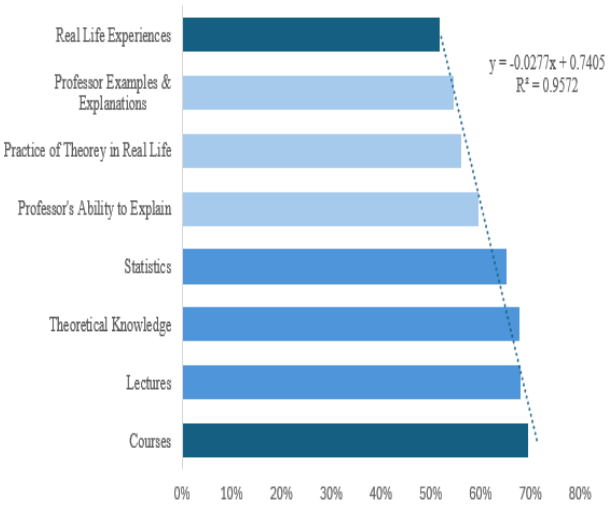


FIGURE V
AVERAGE CROSS-CORRELATION VALUES OF PART A'S DATA

The standard deviations shown in Table I are indicators of how much participants' choices deviated from the standard attained for the associated column value option in Figure IV. The lowest standard deviation in Part A data shown in this table is deduced for statistical knowledge at a rate of 5.98% while the second lowest standard deviation is identified for theoretical knowledge at a rate of 8.97%. The highest standard deviation is determined for real-life experiences of the RP while the second highest standard deviation was attained for practice of theory in real life.

TABLE I
A SUMMARY OF AVERAGE & STANDARD DEVIATIONS OF CROSS-CORRELATIONS

| | Option | (Average, Standard Deviation) in % |
|---|---|---|
| 1 | Courses | (69.52, 11.62) |
| 2 | Lectures | (68.1, 12.3) |
| 3 | Theoretical Knowledge | (67.86, 8.97) |
| 4 | Statistics | (65.14, 5.98) |
| 5 | Professor's Ability to Explain | (59.64, 11.5) |
| 6 | Practice of Theory in Real-life | (56.17, 12.97) |
| 7 | Professor's Examples & Explanations | (54.6, 11.68) |
| 8 | Real-life experience of the student | (51.75, 14.84) |

In conclusion of the quantitative analysis of the data, the top choices that RPs believed to impact their risk assessment ability included their real-life experiences, professor's examples and explanations in the classroom, RPs' practice of the theory in real life, and the professor's ability to explain the theory. Among these participants, at least 94.29% of them happened to either self-experienced or someone around them in the family or friends experienced a cyber-incident. Finally, about 87% of the participants have some sort of anxiety on occasions.

*III. Mann-Whitney and Kruskal-Wallis Tests*

The Mann-Whitney U test is useful for comparing independent data sets as a non-perimetric version of the

Student t-test while the Kruskal-Wallis H-test can be applied on more than two data samples as the non-parametric version of the ANOVA test. In this regard, we use the Mann-Whitney U-test for evaluating the three parts' data sets as three independent samples. Application of the Mann-Whitney U-test on all coupled data sets resulted in statistically significant results indicating that the results are related at a statistically significant level. The Kruskal-Wallis H- test is applied to the three parts altogether that resulted in a p-value of 3.8%. Hence, we can conclude that there is no significant difference in ranking when all the three groups are chosen that confirms the results of Mann-Whitney U test for all three categories' collective analysis.

## QUALITATIVE ANALYSIS AND RESULTS

The qualitative analysis of the data relied on the video recorded and transcribed interview responses of the RPs. The participants are compensated with money for their participation in the interviews with the Principled Investigator (PI). The PI conducted all the interviews with the RPs to furthermore attain information on the RPs' prior responses to the research questions. The qualitative results have a major role in such an understanding of the quantitative results through the integration of the results attained for both types of analysis. Several different examples of the transcribed collected information will be displayed in this section for Parts A-C.

Risk assessment in cybersecurity has a major role in analyzing a variety of risks levels for different cyber-systems. Pedagogically, understanding students' risk assessment levels is essential to build more towards their success. This is the first such a pedagogical attempt to the best of our knowledge. This understanding can help us to build upon not only success levels of students but also improve tomorrow's cybersecurity professionals that are responsible for risk assessments of the systems that we will be using. In addition, cybersecurity students' interest in the field may be driven by the cybersecurity issues that are either by them or the persons around them. Lastly, anxiety is another factor that can impact their success and learning and we investigate furthermore of the associated research's qualitative results with examples provided below.

The following participant's risk assessment responses mainly relied on the importance of examples and course coverage, a family member working as a cybersecurity professional who experienced a cyberattack at his work, and hardly any experience of anxiety during the learning process.

**Interviewer.** *Which of the following factors do you believe impact your ability to assess risk in cybersecurity?*

**RP 1.** *It could be a little bit of my statistical knowledge, it's not a huge part, but I can see how that plays. My knowledge on the theoretical contents from the courses as if there is an example. I don't have any practice of the theory on real life risk assessment applications. Professor's examples and explanations would help a lot to see what type of risk they had to assess during their whole career. Real life examples would be nice. Courses, lectures, and professor's ability to explain. I don't believe that's too much of a deal as long as the professor is explaining it.*

**Interviewer.** *And which one do you think would be the most important factor among these?*

**RP 1.** *I think the lectures because it could be taken from the SANS or from Cisco or something like that and it explains it in a nice professional way written down somewhere. You can look back on your laptop.*

**Interviewer.** *Did you or anyone around you happen to experience any key personal experiences, such as encountering a cybersecurity breach, online privacy concerns, or participation in tech programs in the past that played a role in shaping your interest in a cybersecurity field?*

**RP 1.** I *would say, maybe not too much on my end for the cause. Me and the family members would tie in together my family members and me. Maybe there was an instance of our router shutting down based on a small attack, but I wouldn't say that was too big and at least one of my friends experienced it. My brother has actually experienced it telling me. What goes on? At least not personally. But in his job. I would definitely say that it impacted me because at that time of the small little D dos or DOS attack on my house. I didn't know what was going on and I wanted to gain knowledge about what was going on.*

**Interviewer.** *Does your anxiety levels impact your learning.*

**RP 1** *No, I think, I think sometimes in very rare cases things can get overwhelming. Based on the amount of load work, not just about school, about everything in general. So, it sometimes may impact my learning, but I usually feel as if I'm blessed when it comes to taking tests. I don't overthink too. I'm not the best test taker, but I can manage to take a test, so that's why I say it doesn't impact my learning because. When I take the test, the reflection of the test is based on how hard I worked. So, if I feel as if I worked, studied very hard for a test, I can't get a bad grade.*

The following RP stresses the importance of self-awareness and anxiety levels impacting the RP. In addition, the RP's family members also experienced a cyberattack that impacted the person.

**Interviewer.** *Which of the following factors do you believe impact your ability to assess risk in cybersecurity and looking at these, which ones would you pick?*

**RP 2.** *I'd say self-awareness, or what I'd call status acknowledgment, is really important. It's about always checking in with yourself when you're working on something—asking questions like, Did I do this right? or is there a better, more efficient way to do it? That constant reflection helps you improve. For example, when you're working in labs or practicing on your own, it's not just about completing the task. It's about making sure you're doing it the best way possible. Maybe there's an easier or more powerful method you didn't consider and learning that can make a big difference. So yeah, the key for me is to always evaluate what I've done and look for ways to be more efficient and effective next time. That kind of mindset really helps with assessing risk and improving your skills in cybersecurity. Yeah, I'd also say lectures are really important. Hands-on experience is great, but you need the knowledge to go with it. For example, when a professor explains how to approach something or what's going on, it really builds that foundation. Even if you don't have hands-on experience at that moment, those lectures can still give you the knowledge you need. Like, when the professor says, "This is how we do it," you can take that theoretical understanding and then make sure you're applying it correctly when you practice later. So, combining lectures and status acknowledgment is key. You need both to make sure you're doing things the right way and improving every time. Together, they really help you grow into a well-rounded cybersecurity analyst.*

**Interviewer.** *Did you or anyone around you happen to expense any key personal experiences, such as encountering a cybersecurity breach, online privacy concerns, or participation tech programs in the?*

**RP 2**. *Yeah, actually, my family members had some experiences that really influenced me. A lot of my cousins are software engineers, and they've had some interesting real-life incidents in their work. When they talk about the challenges they've faced—like cybersecurity issues—it's always super motivating for me. In fact, they're the reason I got into the cybersecurity field. I actually started out as a bio major, but one of my cousins encouraged me to take an introductory computing class. I ended up loving it, and that's when I decided to switch my major to cybersecurity. Now, I'm really happy with where I am. I love what I'm studying, and it feels like the right fit for me.*

**Interviewer.** *So, do your anxiety levels impact your learning?*

**RP 2.** *Of course, it does. Like anyone else, when I get anxious, it definitely affects how I learn and solve problems. For example, if I'm working on a technical or cybersecurity problem and I don't get the result I was hoping for, it can be really frustrating. I'm the kind of person who likes to plan things out—I set goals like, "I need to finish this by next week." And if I can't meet that deadline, I start to panic a little. It's especially tough when I'm working on complex problems, and I feel like I'm running out of time. Even though I try my best to get things done by the deadline, if I miss it, my anxiety definitely kicks in and makes it harder to focus. So yeah, I'd say my anxiety level does impact my learning, especially in high-pressure situations. For the exams, yeah, of course, they bring a lot of anxiety too. For example, next week is finals week, and right now we're on a short break. But after just four days off, we're right back at school, and all the finals hit at once. It's a lot to prepare for—every class has a final, and I've got presentations to finish, coding assignments to complete, and so much to study. Even during the break, it doesn't feel like a break because you're grinding every single day to keep up. It definitely pushes the anxiety levels higher, especially when you're juggling so many things at once. But that's just part of the process, I guess.*

The following RP experienced a cyberattack and stated that the risk assessment relates to the professor and the examples given by the professor. The anxiety of the RP occurs sometimes on occasions.

**Interviewer.** *Which of the following factors do you believe impact your ability to assess risk and cybersecurity?*

**RP 3.** *So, I would say professors and examples and explanations because you know there's some professors that you know that are not, you know, maybe giving like a proper examples or estimation of what's going on currently. Maybe they're not, you know, highlighting it as much. That's when it comes to risk in cybersecurity and definitely more of my real-life experience in the risk assessment definitely is impacting a lot of the things I'm doing my day-to-day work, and it's definitely increasing my knowledge when it comes to like assessing risk and I would say definitely my knowledge on theoretical contest in the courses that. What I've learned definitely helps as well and my statistical knowledge as well, that is also another factor. And let's see. And yeah, also the I'll say the courses as well, depending on the courses that I've taken so far, it would apply as well and the professor ability to explain depending on, you know, the risk is another factor.*

**Interviewer.** *Did you or anyone around you happen to experience any key personal experiences, such as encountering a cybersecurity breach, online privacy concerns, or participation in tech programs in the past that played a role in shaping your interest in cybersecurity fields?*

**RP 3.** *Yeah. I would say I personally experienced a data breach that happened in my company like about a couple of months ago. We had a breach that happened and a lot of you know data was lost then we had to recover and after seeing you.*
*Know after seeing that and you know seeing as like you know as our company is growing, the risk is also growing as well as we're getting more you know employees and as you know the database and all our information is increasing. The threat is also. The risk is also increasing and as I you know, I personally experienced that and I've also had friends that also experienced, you know different, you know different, you know, ransomware, different like fishing terms that have happened to them. That like also, you know played a role in my experience.*

**Interviewer.** *Do your anxiety levels impact your learning?*

**RP 3.** *I would say I would say sometimes. When it comes to exams, when it comes to quizzes, you know, when it comes to like, you know, presentation possibly I have to do. So, I would say yes, you know, definitely.*

The qualitative results on Part A's risk assessment related responses focused on the importance of examples that are driven by the professors and the content coverage by the professor as well as the participants' experiences with real-life scenarios. Part B responses had a variety of acknowledgement of cybersecurity issues by the participants but majority of the participants themselves of someone they know experienced such issues. Even if it is not experienced by anyone around them, they stated that they happened to hear either in the news or social media of such incidents.

The responses given to Part C indicated almost all participants' experiencing anxiety during exams and quizzes that impact their learning process. Some of the participants showed high confidence and mentioned no anxiety even during exams or quizzes due to their success levels while some others were not stressed in general unless they don't do well in the classroom.

Overall, the qualitative results agreed with the quantitative results with furthermore justifications and explanations of the participants responses to the research questions.

## CONCLUSIONS AND FUTURE WORK

In this IRB approved study in a university located in Northeastern side of the United States we collected data from 101 students to investigate the factors that they believe to impact their ability to assess risk in cybersecurity, anxiety levels, and cyber-issues experienced by them or someone around them in three parts. The quantitative data analysis relied on statistical analysis, mathematical model fitting, correlation with heatmap evaluations, cross-correlations, and Mann-Whitney U- and Kruskal-Wallis H-tests. The qualitative analysis consisted of transcribed video recordings of the participants that aimed to better understand their research question responses. The participants are compensated money for their participation in the video recorded interviews that are transcribed for furthermore analysis of their initial responses to the research questions. Figure VI demonstrates a summary of the statistics and categories that the cybersecurity students chose for Part A.

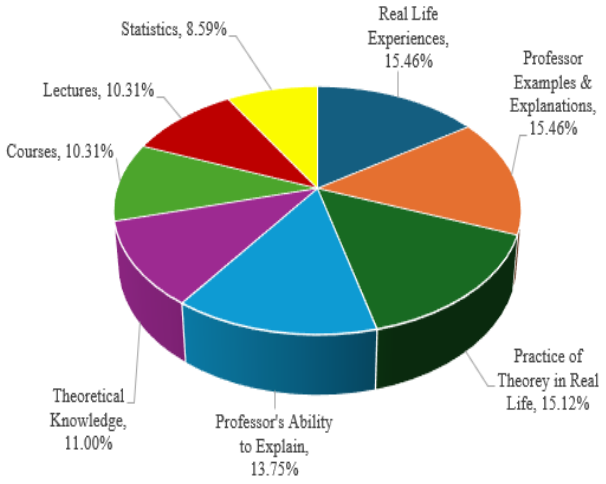


FIGURE VI
DATA DISTRIBUTION OF PART A RESPONSES

Integrated quantitative and qualitative analysis resulted in the following general outcomes:

- The quantitative analysis of the data, the top choices that RPs believed to impact their risk assessment ability included their real-life experiences, professor's examples and explanations in the classroom, RPs' practice of the theory in real life, and the professor's ability to explain the theory. Among these participants, at least 94.29% of them happened to either self-experienced or someone around them in the family or friends experienced a cyber-incident. Finally, about 87% of the participants have some sort of anxiety on occasions.
- Part A's qualitative analysis resulted in examples that are driven by the professors and the content coverage by the professor as well as the participants' experiences with real-life scenarios.
- Qualitative responses to Part B included a variety of acknowledgement of cybersecurity issues by the participants but the majority of the participants themselves of someone they know experienced such issues. Even if it is not experienced by anyone around them, they stated that they happened to hear either in the news or social media of such incidents.
- Responses given to Part C indicated almost all participants' experiencing anxiety during exams and quizzes that impact their learning process. Some of the participants showed high confidence and mentioned no anxiety even during exams or quizzes due to their success levels while some others were not stressed in general unless they do not do well in the classroom.
- Overall, the qualitative results agreed with the quantitative results with furthermore justifications and explanations of the participants responses to the research questions.

Other researchers and educators are also invited to invest time and energy in the analysis of the relevant issues. The results attained in this research can be further used for improving not only the cybersecurity classroom environment but also improving our educational methods and course designs by incorporating the students in the development of courses.

## REFERENCES

[1] Rosta, G., Bottyan, L., & Bognar, L. (2024). On the Factors of Students' Cybersecurity Behavior. PedActa, 14(1).

[2] Ganesen, R., Bakar, A. A., Ramli, R., Rahim, F. A., & Zawawi, M. N. A. (2022). Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions. International Journal of Advanced Computer Science and Applications, 13(8).

[3] Alammari, A., Sohaib, O., & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. PeerJ Computer Science, 8, e827.

[4] Kam, H. J., & Katerattanakul, P. (2019). Enhancing student learning in cybersecurity education using an out-of-class learning approach. Journal of Information Technology Education. Innovations in Practice, 18, 29.

[5] Azzeh, M., Altamimi, A. M., Albashayreh, M., & Al-Oudat, M. A. (2022). Adopting the Cybersecurity Concepts into Curriculum The Potential Effects on Students Cybersecurity Knowledge. *arXiv preprint arXiv:2209.10407*.

[6] Bognár, L., & Bottyán, L. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. *Education Sciences*, *14*(6), 588.

## AUTHOR INFORMATION

**Emre Tokgoz,** Professor, Department of Computer Security, New York State University at Farmingdale, Long Island, NY.

**Joel Joseph,** Research Assistant, Department of Computer Security, New York State University at Farmingdale, Long Island, NY.

**Sergio Duarte,** Research Assistant, Department of Computer Security, New York State University at Farmingdale, Long Island, NY.

**Alyssa Xiang,** Research Assistant, Department of Computer Security, New York State University at Farmingdale, Long Island, NY.

**Julissa Molina,** Research Assistant, Department of Computer Security, New York State University at Farmingdale, Long Island, NY.

**Tanvir Ahmed,** Research Assistant, Department of Computer Security, New York State University at Farmingdale, Long Island, NY.