Teaching Empirical Social-Science Research to Cybersecurity Students: The Case of “Thinking Like a Thief”

Susanne Barth | University of Twente
Pieter Hartel | Delft University of Technology and University of Twente
Marianne Junger and Lorena Montoya | University of Twente

We report on an educational experiment in which computer science master students performed empirical research regarding the human factor in cybersecurity.

Cybersecurity is a multidisciplinary field straddling the technical and the social sciences. Accordingly, cybersecurity students learn about the role the human factor plays in cybersecurity. For the cybersecurity program of the federation of the four Dutch technical universities (Delft University of Technology, Eindhoven University of Technology, the University of Twente, and Wageningen University and Research Centre; 4TU; https://www.4tu.nl/cybsec/), we developed and taught a course on the human factor in cybersecurity. We based the content of the course on the principles of crime science because that field is focused on making use of empirical research in countering crime. The aim of crime science is to be relevant for practice, to study crime and test interventions, with the aim of developing policies that improve context and decrease the opportunities for crime. We believe that an emphasis on empirical social-science research can be particularly fruitful for students as they enter cybersecurity careers.

In both crime science and cybersecurity, “thinking like a thief” often leads to insights. In the computing literature, this is called adversarial thinking. It is the offender who is looking for ways to misuse a design; hence, the prudent designer is well advised to also think like a thief. An illustration of what this might entail is the ordinary beer glass, which, when broken, becomes a lethal weapon. Hence, a designer who has been thinking like a thief uses laminated glass that does not break. This example highlights not only the approach shift but also the multidisciplinary method used in crime science.

Cybersecurity curricula across the world offer a variety of courses on adversarial thinking. However, most cybersecurity courses focus on the technical aspects of adversarial thinking, such as cryptanalysis (mathematics), kernel hacking (systems), and red–blue teaming (networks). In almost all courses that take the human factor into account, the students are either pitted against each other or work in a laboratory setting. We believe that realistic settings significantly improve the learning experience. There is, of course, a good reason to make students work in a laboratory: the ethical and legal issues of real research are thorny and time consuming.

The students in our course are asked to conduct and document a real experiment in the real world. This requires our students to seek approval for their research proposal from the University of Twente’s IRB. Students acquire valuable experience by going through the process of interacting with the IRB. We have found no reports in the computing literature on courses that similarly provide students with first-hand experience of working with an IRB.

Performing realistic empirical social-science research with high-quality results gives the students the best possible learning experience. However, if the results are disappointing, the learning experience will be poor. Therefore, we set out to investigate—and, if possible, control—factors influencing the quality of the student work.
The quality-influencing factors that we considered were 1) the amount of time available for the course, 2) factors that the teachers control, 3) factors that the students control, and 4) factors that neither control. The indicators of the quality of the student work that we considered were 1) random allocation of subjects, 2) statistically significant results, and 3) publication quality of the papers. More specifically, we were interested in answering the following questions:

1. Is a learning-by-doing course, in the form of an experimental design with high-quality results, manageable within five European credits (ECs; 140 student hours)?
2. How do factors that the teachers control, such as improvements to the course content over the years, influence the quality of the results?
3. How do factors that the students control, such as choice of research methods and topics, influence the quality of the results?
4. How do factors that neither the teachers nor the students control, such as group diversity, influence the quality of the results?

To answer these questions, we analyzed the student papers, examined surveys completed by the students, and interviewed the students.

Learning-by-Doing Course
Our cybercrime-science course is a five-EC (140 student hours), one-semester course for computer-science master students specializing in cybersecurity. The learning outcomes of the course are

- a good understanding of the theoretical principles of crime science
- a good understanding of the psychological issues of cybersecurity
- an appreciation of the spectrum of different cybercrimes
- skills necessary to research cybercrime-prevention measures.

Throughout the course, the students work toward a conference where they present a research paper on a topic of their choice. Assessment is done entirely by peer review, moderated by the lecturers.

During the first eight weeks, students attend weekly lectures on crime science, cybercrime, and social-science research methods. At the same time, teams of students—normally three students per team—each draft a research proposal for a cybercrime-prevention project of their choice. Students are free to choose a topic for their research. After two rounds of feedback by their peers and lecturers on the research proposals, the teams submit their projects to the IRB. In cases where deception is involved, the students often have to modify their proposals. If the IRB refuses permission, students must develop alternatives.

Upon approval of the IRB, the students execute their projects, leading to the preparation of a six-page paper based on the American Psychological Association guidelines. The papers are presented at a half-day conference at the end of the semester. The students peer-review each other’s papers and presentations. This process is moderated by the lecturers. Finally, the students complete a questionnaire on their experience. The first aim of this article is to describe students’ studies and some global evaluations. In addition, we test some hypotheses.

Improvements to the Course Contents
During the early years of the course, we found that computer-science students needed more help than we had anticipated in performing social-science research. In subsequent course iterations, we increased the number of lectures about social-science research methods and decreased the number of lectures about other topics. We also introduced clinics where students could get advice. Thus, we changed from a passive to a more active, trouble-shooting form of delivering social-science research methods. We were interested in the extent to which our cybersecurity students apply standard social-science research methods.15 Do students use random selection of subjects for the control group? Do they analyze the data and check for statistically significant results? The second aim of our research for this article was therefore to find out whether there are differences between the papers of the first three years compared to those of the last three years reflecting the increased focus on the social perspective.

Choice of Research Method and Topic
Since crime science emphasizes experimental work, we explicitly encouraged students to develop their own intervention and to test it in an experiment. Thus, the third aim of this article is to examine whether the topics chosen by students involved an experiment or a survey.

Group Diversity
Group diversity plays an important role in education. Since our students are free to choose their teammates, we thought that group diversity might explain some of the performance differences among the teams. Studies have shown that gender stereotypes and national and cultural differences can affect collaborative learning. In research for this article, we have assumed that gender and nationality are acceptable proxies for group diversity. There are no significant language
differences in the 4TU master program as the teaching language is English in a non-English-speaking country. Accordingly, the final aim of this article is to investigate differences between homogeneous male teams and teams that include at least one female student as well as differences between homogeneous Dutch teams and teams that include at least one international student. International students from many countries around the world make up about 30% of the student population of the 4TU master course.

Method
To measure the factors that influence the quality of the student work and of the work itself, we collected three data sets. The first data set consists of the research papers written by student teams. The next set includes the course-evaluation questionnaires completed by students who attended the course. The last data set contains a few structured interviews with students who completed the course. The IRB of the faculty of Electrical Engineering, Mathematics, and Computer Science at the University of Twente approved the present study.

Student Papers
The student papers were coded using three independent variables (gender, nationality, and year) and four dependent variables (applied research method, sample randomization, statistical significance tests, and chosen research topic).

The background of the students was coded as follows:

- The gender was coded as zero when at least one female participated in the group and one when the group consisted of males only.
- The nationality was coded as zero when at least one international student participated in the group and one when the group consisted of Dutch students only.
- The year was coded as zero for the early years (2012–2014), and one for later years (2014–2016).

The quality of the results was coded as follows:

- The method was coded as zero for a survey and one when students performed an experiment to test an intervention.
- The randomization was coded as zero when the student researchers assigned the subjects to the control group, one when they had not controlled the subject assignment, and two in the case of surveys, i.e. not applicable.
- The statistical-significance tests were coded as zero when significant results were reported; one when the student researchers argued either that no significant results would be possible, typically due to a limited data set, or that no significant results were found; and two when no statistical analysis had been performed.

The fourth dependent variable describing the topics of the papers was coded as follows:

- Projects on illegal-activity reduction were coded as zero. This required the subjects to engage in simulated illegal activity, such as illegal downloading, littering, illegal parking, or using fake IDs.
- Studies on password-usability improvement were coded as four. This required subjects to select, enter, remember, or recover passwords.
- Research on raising awareness of phishing risks were coded as two.
- Studies on raising awareness of privacy risks were coded as three. These studies required subjects to interact (via such means as email, Facebook, face-to-face meetings, brain–computer interfaces, web cams, geotagged photos, or QR codes) using hardware or software provided by the student researchers.
- Research on raising awareness of security risks were coded as four. This required subjects to interact with hardware or software that has been deliberately mismanaged. Examples include wireless access points, drive-by-download websites, fake login screens, Facebook advertisements, phone-charging stations, unattended laptops, out-of-date software, and lost USB sticks.
- Studies of threat assessments were coded as five. To demonstrate to what extent it is possible to use the information for illegal purposes, subjects were asked to surrender information via a variety of methods, such as with Tor exit nodes to de-anonymize traffic, Wi-Fi access points to access them illegally, Wi-Fi-enabled devices to break into homes, online social sports sites to break into homes, online sources to obtain sensitive information for blackmail, or online sources to create fake IDs.
- Studies of victimization were coded as six. In these projects, the subjects are targets of a form of cybercrime, such as harassment, or ransomware.

Student Surveys
At the end of the course, students were asked to complete a course-evaluation questionnaire. For the wording of the survey questions, we took as our model the Intrinsic Motivation Inventory scale (IMI). 6 We did not use the IMI scale itself, as we did not want to overwhelm our students with questions, and we reworded the questions to better suit our study. As with the IMI scale, the subjects were asked to indicate on a five-point scale (from five: strongly disagree; to one: strongly agree) their level of agreement on a set of propositions
(the numbers in parentheses refer to the corresponding IMI items):

- I had sleepless nights for fear of our experiment going wrong. (11)
- I had to work harder than average on the course. (3)
- The course has increased my interest in social-science research. (8)
- I am confident that, during my career, I will be using what I have learned during the course. (14)
- I will never forget the course. (4)
- I had a lot of fun doing the experiment. (7)
- I am less likely to fall for a social-engineering attack. (This is not related to the IMI scale because this is not a motivation.)

The independent variables were coded as described in the section “Student Papers.”

Student Interviews
We invited all 30 students who attended the last version of the course for a one-hour structured face-to-face interview. Because the main purpose of the interview was to investigate the effect of diversity on student performance, we wanted to give the interviewees some guidance. For this, we used the six factors of the Intercultural Effectiveness Scale (IES). These factors are as follows:

- the ability to adapt to new situations (e.g., feeling comfortable/uncomfortable while interacting with people from other cultures)
- foreign-language skills (e.g., proper use of English language)
- distance (e.g., difficulty or ease in interacting with people from other cultures)
- expression (e.g., difficulty or ease in following conversations in a foreign language)
- respect (e.g., ability to pay attention to cultural differences while interacting with people from other cultures)
- being relaxed (e.g., feeling relaxed while interacting with people from other cultures).

We printed the given description of each factor on a card and placed the six cards before the interviewee. We asked the interviewees eight open questions focusing on decision making within their student teams. We asked why these decisions were made and whether the six IES factors had played a role in the decision-making process. The questions we asked the students were as follows:

- Which nationalities were represented in your team (including your own)?
- Which topic did your team choose?
- Did your team decide to conduct a survey or an experiment?
- Did your team decide to analyze the statistical significance of the data?
- Did your teamwork influence your interest in social-science research?
- Did working on the team influence your ability to withstand social-engineering attacks?
- Is there anything else that you would like to mention about your experience on the team?

The interviews were recorded, and each interviewee received €10 for his or her time.

Results

Learning-by-Doing Course
An analysis of the student papers shows that, over six years, 196 students (158 male, 38 female; 124 Dutch, 72 international) wrote 72 papers (44 experiments, 28 surveys) in teams of usually three students but sometimes two and, in one case, four. In each academic year, students produced between eight and 19 papers: 29 in the first three years and 43 in the last three years. One study was based on only \( N = 4 \) subjects, and the maximum number of subjects was \( N = 762 \). From the 72 teams, 28 teams contained at least one female, and 38 teams contained at least one international student. Phishing was the topic chosen most often (27.8%), followed by security awareness (25%) and the usability of passwords (13.9%). Reduction of illegal behavior and privacy awareness were both chosen by 11.1% of the teams. Threat assessments (8.3%) and victimization studies (2.8%) were least likely to be chosen. All papers were coded by one of the authors of this article. Seven papers (10%), chosen at random, were also coded by a second author of this article. Of the 49 items from those seven papers (i.e., seven papers \( \times \) seven variables), the two coders had different opinions on four items (8%). After discussion, the two coders agreed that the differences were all due to coding errors and not to different understanding about these items.

An analysis of the student surveys shows that, over six years, 124 students (100 male, 24 female) out of the total population of 196 students (response rate: 63.2%) completed our survey. The majority were Dutch (65.9%). The international students originated from 34 countries around the world. The respondents of the surveys did not agree or strongly agree with the first two propositions: 64.5% of the students reported that they did not have sleepless nights, and 54.8%
reported that they did not work harder than in other courses. The students agreed or strongly agreed on the remaining propositions. For 52.4% of the students, the course raised interest in social-science research, 56.5% felt that they expected to be using what they had learned in their career, 60.5% would not easily forget the course, 62.9% had fun, and 47.6% felt themselves now better prepared to face social-engineering threats. Cronbach’s alpha for the seven-item scale from the survey was 0.7, showing that our combined measure is reliable.

Of the 10 teams taking part in the last version of the course, representatives of four teams agreed to be interviewed (40%). Two interviewees represented all-male, all-Dutch teams, and two interviewees represented teams with at least one international student. One of the interviewees was female.

**Improvements to the Course Contents**

An analysis of the student papers shows that students taking the course over the last three years investigated statistical significance more often than did students who took the course in the first three years (Table 1). This was a significant result. Students also randomized the control group more often in later years, but this was not statistically significant.

An analysis of the student surveys shows that the opinion of the students on the course did not differ significantly year by year with one exception. Table 2 shows that students who took the course in recent years were more likely than students who took the course early on to think they would fall for social-engineering attacks. The student interviews did not provide new insights into the improvements of the course over the years.

**Choice of Research Method and Topic**

An analysis of the student papers shows that there was a significant relationship between the chosen topic and the research method used (Table 3). Some topics were studied more often using experiments (e.g., phishing) and some more often through surveys (e.g., threat assessments). Table 4 shows that in recent years the number of experiments increased, and the number of surveys decreased. This was a significant finding.

![Table 1. The percentage of student studies that were statistically significant: a comparison of studies in the first three years the course was offered versus the last three years.](image1)

<table>
<thead>
<tr>
<th>Statistically significant results have been found.</th>
<th>First three years</th>
<th>Last three years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>23.3%</td>
<td>44.8%</td>
</tr>
<tr>
<td>No</td>
<td>25.6%</td>
<td>41.4%</td>
</tr>
<tr>
<td>Not investigated</td>
<td>51.2%</td>
<td>13.8%</td>
</tr>
<tr>
<td>N</td>
<td>43</td>
<td>29</td>
</tr>
</tbody>
</table>

Chi-square = 10.6, df = 2, p = 0.005.

![Table 2. Susceptibility to social-engineering attack: a comparison of responses from students who took the course in the first three years the course was offered versus responses from students who took the course in the last three years.](image2)

<table>
<thead>
<tr>
<th>I am less likely to fall for a social-engineering attack.</th>
<th>First three years</th>
<th>Last three years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree or agree</td>
<td>52.8%</td>
<td>34.4%</td>
</tr>
<tr>
<td>Neutral</td>
<td>16.9%</td>
<td>34.4%</td>
</tr>
<tr>
<td>Strongly disagree or disagree</td>
<td>30.3%</td>
<td>31.4%</td>
</tr>
<tr>
<td>N</td>
<td>89</td>
<td>35</td>
</tr>
</tbody>
</table>

Chi-square = 5.3, df = 2, p = 0.070.

![Table 3. Choice of topic by research method.](image3)

<table>
<thead>
<tr>
<th>Choice of topic</th>
<th>Survey</th>
<th>Experiment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce tendency to illegal activity</td>
<td>3.7%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Study or improve the usability of passwords</td>
<td>18.5%</td>
<td>11.1%</td>
</tr>
<tr>
<td>Increase awareness of phishing risks</td>
<td>14.8%</td>
<td>35.6%</td>
</tr>
<tr>
<td>Increase awareness of privacy risks</td>
<td>11.1%</td>
<td>11.1%</td>
</tr>
<tr>
<td>Increase awareness of security risks</td>
<td>25.9%</td>
<td>24.4%</td>
</tr>
<tr>
<td>Threat assessments</td>
<td>18.5%</td>
<td>2.2%</td>
</tr>
<tr>
<td>Victimization studies</td>
<td>7.4%</td>
<td>0.0%</td>
</tr>
<tr>
<td>N</td>
<td>27</td>
<td>45</td>
</tr>
</tbody>
</table>

Chi-square = 14.1, df = 6, p = 0.028.
student surveys and interviews did not provide new insights into the choice of research method and topic.

**Group Diversity**
The analysis of the student papers also indicated that there were no significant differences by gender or nationality. The only point worth noting is that all-male, all-Dutch groups carried out all six threat assessments.

An analysis of the surveys indicated that gender or nationality differences did not significantly influence student opinion scales with one exception: international students reported that their interest in social-science research had increased, but Dutch students reported no such increase in interest (Table 5).

An analysis of the interviews shed light on group-diversity issues. The interviewees agreed that the six IES factors had more influence on the interaction between the team and their subjects than on the team itself. In particular, all interviewed teams gave considerable attention to formulating their questionnaires, briefings, and informed-consent forms in plain English and sometimes also in plain Dutch. The IES factors did not influence the decision making of the teams, with one exception: the only native English speaker in the class used a more elaborate form of English than his teammates could handle. During the interviews, students stated that cultural factors did not affect them or the way their group functioned.

**Discussion**

**Learning-by-Doing Course**

Three of the student papers contained original ideas striking enough to be published after a thorough revision:

- The first paper, by two Dutch students, showed how easy it is to discover the home address of subjects from their web presence. Thinking like a thief, the students hypothesized that people are more likely to “leave their tracks” on a social sports site if they feel proud of an achievement. The students collected the Runkeeper (https://runkeeper.com) profile of 304 subjects and calculated the home address from the tracks of each runner shown on the website. Since most people start running from home, and stop running to cool down close to home, the address could be determined accurately in most cases. The students then tried to obtain the home address from other sources as well, such as the Facebook profile of the runners. Discovering the home address from Runkeeper profiles was twice as successful as from Facebook. This work has been revised by one of the supervisors and was published in a scientific journal.

- The second paper, by one international and two Dutch students, researched the effect of antiphishing training on 159 schoolchildren between nine and 12 years old. There was a statistically significant difference between the experimental group, which received training, and the control group, which did not receive training. This work was revised by one of our Ph.D. students and won the Distinguished Paper Award at the 2017 Association for Computing Machinery Symposium on Usable Privacy and Security.

- The third paper, by three Dutch students, described an experiment where passersby on one of the main squares in a small city were approached to participate in a survey. Subjects were randomly assigned to the control group (25 subjects) or the experimental group (22 subjects). The survey for the experimental group included some questions designed to raise awareness about phishing. Subjects in the experimental group

---

**Table 4. Surveys versus experiments: a comparison of research methods chosen by students who took the course in the first three years it was offered versus methods chosen by those who took the course in the last three years.**

<table>
<thead>
<tr>
<th>Applied research method</th>
<th>First three years</th>
<th>Last three years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey</td>
<td>46.5%</td>
<td>27.6%</td>
</tr>
<tr>
<td>Experiment</td>
<td>53.5%</td>
<td>72.4%</td>
</tr>
<tr>
<td>N</td>
<td>43</td>
<td>29</td>
</tr>
</tbody>
</table>

Chi-square = 2.6, df = 1, p = 0.011.

**Table 5. Increased interest in social-science research: a comparison of responses from international students versus Dutch students.**

<table>
<thead>
<tr>
<th>The course has increased my interest in social science research.</th>
<th>International students</th>
<th>Dutch students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>77.5%</td>
<td>40.2%</td>
</tr>
<tr>
<td>Neither agree nor disagree</td>
<td>17.5%</td>
<td>34.1%</td>
</tr>
<tr>
<td>Disagree</td>
<td>5.0%</td>
<td>25.6%</td>
</tr>
<tr>
<td>N</td>
<td>40</td>
<td>82</td>
</tr>
</tbody>
</table>

Chi-square = 15.8, df = 2, p < 0.005.
did significantly better than those in the control group. A student not involved in the original work collected a new data set, analyzed the results, and rewrote the paper. The paper was published in a scientific journal with an International Scientific Indexing impact factor of 3.435.

The publication of these three papers demonstrates that students can master social-science research skills and apply them to crime prevention. The three published papers were innovative, and one was even worthy of an award at the top conference in the field. The three papers also prove that it is not only feasible to allow students to perform experiments in the real world but that this may lead to high-quality results as well. With proper guidance and sufficient revision, computer-science master students are indeed able to conduct research during a five-EC course that is worthy of publication. We believe that the learning experience with such a result is tremendous.

Improvements to the Course Contents

Students researchers who took the course in the last three years performed more experiments and analyzed the statistical significance more often than their counterparts who took the course in the first three years. These differences are significant. Hence, we conclude that the delivery of social-science research methods improved over the years.

What has deteriorated is the self-reported ability of the students to resist social engineering. This difference is also significant. We think that the two changes are related. Shifting the attention from crime-science to social-science research methodology also diverts the attention from the main tool employed by offenders: social engineering. The challenge, therefore, is to maintain a good balance between content and form. We are trying to achieve this by explicitly commenting on methodological issues when we present cybercrime studies from the literature in our lectures.

Choice of Research Method and Topic

Consistent with the course aims, the number of experiments (44) exceeded the number of surveys (28). This is a significant finding. It indicates that within the constraints of a one-semester, five-EC course, it is possible to perform a cybercrime-prevention experiment from start to finish.

Some topics were studied more often in experiments (phishing) and some more often in surveys (threat assessments); this was a significant finding. While, in principle, all topics are amenable to experimentation, doing so within the time constraints of a one-semester course remains a challenge.

The students who were interviewed wanted to develop an intervention and conduct a proper experiment to measure objectively whether the intervention worked. They did not consider a survey as rewarding. One of the interviewees stated, “Surveys are boring. It’s difficult to get the sample. Field experiments help you to find out what the problem is in the real world.”

One interviewee explained that the choice of topic requires considerable time and dedication. He stated that his teammates had opposing views on a specific technology: two-factor authentication (2FA). Some team members used 2FA all of the time, and some never. The team decided to study whether the population at large also held opposing views. We believe that it is important to allow the students sufficient time to choose a topic in which they are all genuinely interested.

Group Diversity

There were no significant differences by gender or nationality on team performance. Also, in the interviews, students were of the opinion that cultural factors did not affect them or the way their group functioned. Instead, students indicated that different skill levels were relevant. One of the interviewees stated, “The different skill sets in the team were a factor. One person did not have any data-analysis skills. The cultural differences did not have an influence.”

International students reported that their interest in social-science research had increased, but Dutch students did not; this difference is statistically significant. The course did not include any training to withstand social engineering, so an improved resilience to social engineering cannot be due to the course material. The interviewees said they learned a lot about social engineering from the work of their peers. One of the interviewees commented, “The experience made me realize that a lot of people around me do not understand that social engineering is a valid attack vector. That was a very good education experience.”
We believe that our international students are well adapted to the way of working in The Netherlands because most of them have been in the country for at least half a year and some considerably longer.

**Limitations**

The subjects of this study were 196 students from four Dutch universities. Most of the students were Dutch, but the international students from 34 different countries represented a large minority. The size of this study was thus moderate. Our results may not be representative for all countries and for all higher-education organizations due to the international nature of the university where the study was carried out. We used a small subset of the items of the IMI scale, which does not necessarily preserve the validity of the scale.

One of the limitations of teaching-related research is that the students are also subjects of this study and the lecturers are also researchers of this study. To reduce the risk of answers skewed to please or impress researchers, the surveys and interviews were all performed after the students received their marks.

The main lessons we learned were as follows:

- It is possible, within a five-EC, one-semester course, for computer-science students to conduct social-science research that lays the foundation for high-quality papers suitable for publication. Three of the 72 student papers were eventually published after heavy revision.
- Giving students the freedom to choose the topic they wish to research creates a stimulating learning experience.
- Gender and nationality differences had no significant effect on student performance.
- Teaching engineers about social-science research methods broadens the students’ view, as it forces them to consider the point of view of others rather than just their own or those of their immediate peers.
- Having students peer review each other’s work, with the final mark determined by peer review (moderated by the lecturers), is more effective than traditional lecturer–student interactions in helping students learn.

We offer the following recommendations for teachers of similar courses:

- Include social-science research methods in a cybersecurity curriculum, as cybersecurity professionals must deal with the human factor. Ideally, this should be a separate course, but a combination with a course like ours that focuses on cybercrime is an acceptable alternative.
- Because students have complete freedom to choose their own research topic, projects can vary a lot. Accordingly, personal attention is important. Therefore, we suggest providing regular feedback to the students on their progress. This can be done by, for example, hiring teaching assistants with a social-science background who regularly meet with each student team separately. We believe this is important to make each study a success.
- A course on social-science research methods should include an experiment where the students themselves are the subjects. This will help them understand the fine points of research ethics.
- To avoid unnecessary delays, discuss the student proposals with a representative of the IRB before the students submit their proposals.
- Provide the students with checklists to make sure they remember to provide the IRB with every relevant detail.
- Smooth the path through the IRB by preparing a small set of standard applications, such as an online survey, an awareness campaign, and a usability study. Most students will then be able to follow a standard approach and avoid common mistakes.
- Work with the IRB to implement a fast-track procedure for approval of standard experiments to maximize available time and reduce the burden on institutional ethical bodies.
- Create an inventory of logistical mishaps from previous experiments to increase the probability of success for new experiments.

After six iterations, we are still keen to improve our course. We are considering several possible changes:

- Students generally prefer to select their own teammates. This tends to create homogeneous groups, which, according to the literature, can be less creative than nonhomogeneous groups. We are looking for ways promote group diversity without annoying the students.
- We would like to better integrate the cybercrime teaching with the social-science research methods. For example, we are explicitly commenting on the research method when we discuss cybercrime studies from the literature.
- Some studies are harder to do with informed consent than without, because signing the informed consent may bias the subject. We are looking for ways to reduce the risk of bias.

We hope that this article will help others with similar aims, and that we hear from other teachers who have solved similar problems.
References


Susanne Barth is a Ph.D. candidate at the University of Twente. Her research interests are cybersecurity and privacy, and usability testing. Barth received an M.S. in communication science with a specialization in marketing and an M.S. in psychology with a specialization in human factors and media psychology from the University of Twente. Contact her at s.barth@utwente.nl.

Pieter Hartel is professor of cybersecurity at Delft University of Technology and the University of Twente. His research interests are crime science, cybercrime, and block-chain technology. Hartel received a Ph.D. in computer science from the University of Amsterdam. Contact him at pieter.hartel@tudelft.nl.

Marianne Junger is professor of cybersecurity and business at the University of Twente. Her research interests are crime science, cybercrime, and the human factor. Junger received a Ph.D. from the Department of Law of the Free University of Amsterdam. Contact her at m.junger@utwente.nl.

Lorena Montoya is coordinator of the Graduate School at the University of Twente. Her research interests are risks in general and crime prevention and disaster management in particular. Montoya received a Ph.D. in risk management from the University of Utrecht. Contact her a.l.montoya@utwente.nl.